Army Research Laboratory

Vulnerability Risk Assessment

by
Gary L. Guzie

Survivability/Lethality Analysis Directorate
Information & Electronic Protection Division

ARL-TR-1045

June 2000

NOTICES

Disclaimers

The findings in this report are not to be construed as an official Department of the Army position, unless so designated by other authorized documents.

The citation of trade names and names of manufacturers in this report is not to be construed as official Government endorsement or approval of commercial products or services referenced herein.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY (*Leave Blank*)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	June 2000	Final

4. TITLE AND SUBTITLE
Vulnerability Risk Assessment

5. FUNDING NUMBERS

6. AUTHOR(S)
Gary L. Guzie

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
US Army Research Laboratory
Survivability/Lethality Analysis Directorate
Attn: AMSRL-SL-EA
White Sands Missile Range NM 88002-5513

8. PERFORMING ORGANIZATION REPORT NUMBER
ARL-TR-1045

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
US Army Research Laboratory
2800 Powder Mill Road
Adelphi MD 20783-1145

10. SPONSORING/MONITORING AGENCY REPORT NUMBER
ARL-TR-1045

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION/AVAILABILITY STATEMENT
Distribution is unlimited.

12b. DISTRIBUTION CODE

13. ABSTRACT (Maximum 200 words)
This report describes a methodology that provides a practical and simple process for applying classical risk analysis/assessment theory to the vulnerability analysis/assessment of military systems in particular and generally to any hazard analysis desired. It applies to both weapon effects and countermeasure effects equivalently as well as to operational environment effects (natural and man-made), for the first time providing system analysts with a common/unified vulnerability assessment methodology for these diverse areas. This new vulnerability risk analysis/assessment methodology also identifies and corrects procedural errors in the traditional hazard risk analysis charts used for safety/health and many other risk assessment programs.

14. SUBJECT TERMS
vulnerability assessment, survivability, lethality, risk analysis, effectiveness analysis

15. NUMBER OF PAGES
67

16. PRICE CODE

17. SECURITY CLASSIFICATION OF THIS REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	SAR

Preface

The purpose of this report is to describe a methodology that provides a practical and simple process for applying classical *risk analysis/assessment* theory to the *vulnerability analysis/assessment* of military systems in particular and generally to any hazard analysis desired. It applies to both *physical "hard kill"* weapons effects and *functional "soft kill"* countermeasures effects as well as to operational environment effects (natural and man-made), for the first time providing system analysts with a common/unified vulnerability assessment methodology for these diverse areas. This new vulnerability risk analysis/assessment methodology also identifies and corrects procedural errors in the traditional hazard risk analysis charts used for safety/health and many other risk assessment programs.

This new methodology is applicable to all risk analysis programs conducted by the materiel development and evaluation communities and can also be used to develop initial threat and system requirements prioritizations by the combat development community. It has attributes that make it powerful in its simplicity yet thorough in its approach even for complex systems.

Contents

Figures

Executive Summary

Introduction

Department of Defense (DoD) acquisition regulations require critical military programs to employ and be guided by risk management techniques that continuously assess and track the technical and programmatic/financial risks to system development and employment. However, no universally adopted methodology for vulnerability risk assessment has been employed since existing techniques do not provide an adequate and reasonably supportable quantitative or qualitative basis for appropriately determining risk levels.

Purpose/Objective

The purpose of this report is to describe a methodology that provides a practical and simple process for applying classical *risk analysis/assessment* theory to the *vulnerability analysis/assessment* of military systems in particular and generally to any hazard analysis desired. It applies to both *physical "hard kill"* weapons effects and *functional "soft kill"* countermeasures effects as well as to operational environment effects (natural and man-made), for the first time providing system analysts with a common/unified vulnerability assessment methodology for these diverse areas. This new vulnerability risk analysis/assessment methodology also identifies and corrects procedural errors in the traditional hazard risk analysis charts used for safety/health and many other risk assessment programs and incorporates a complementary confidence rating system. [1]

This new methodology is applicable to all risk analysis programs conducted by the materiel development and evaluation communities and can also be used to develop initial threat and system requirements prioritizations by the combat development community. It has attributes that make it powerful in its simplicity yet thorough in its approach even for complex systems.

Overview

The existing definitions for survivability and vulnerability are presented and examined. The procedures commonly used for hazard risk analysis are analyzed and modified to correct inherent errors in the risk level assignments and to provide a basic structure applicable to vulnerability risk analysis. The basic structure and similarity of FMECA risk analysis is discussed. New probability-based definitions for susceptibility, vulnerability, and survivability are presented which are oriented toward critical engagement event probabilities and critical function performance probabilities. The risk matrix and risk analysis charts associated with the equations are described. The vulnerability risk analysis technique's utility for the performance of parameter variation sensitivity analysis is presented. Its utility for performing comparator integrated threat spectrum analysis is also presented. The methodology's application to lethality analysis

and traditional effectiveness analysis is described. The associated topics of risk confidence and risk tolerance and their relative impact on risk analysis are discussed.

Conclusions and Recommendations

The vulnerability risk assessment methodology presented provides a new and improved process to address the critical area of military system survivability analysis, unifying the fields of *risk analysis* and *vulnerability assessment* and providing a common/unified approach to address vulnerability to both *physical "hard kill"* weapon effects and *functional "soft kill"* countermeasure effects. It also provides a more robust and exact methodology for hazard risk assessment and an associated top-level *confidence assessment* procedure. The application of this methodology has the potential to impact the amount of time and funding expended on unnecessary system "gold plating" to meet hostile threats and/or operational environment hazards previously inaccurately assessed as having higher risk levels.

This methodology coincidentally provides a unique and user-friendly audit trail for tracking the status of both the overall risk and the individual contributing risk components/factors as a function of time as system and threat changes occur. Another important attribute is its capability to facilitate the determination of vulnerability risk assessment *sensitivity to threat/hazard parameter variations* and to thereby augment the evaluation community's ability to project realistic and reasonable threat vulnerability risks.

It is recommended that this new and improved risk analysis/assessment methodology be officially adopted and applied uniformly and universally to all hostile threat and operational environment hazard (natural and man-made, intentional and non-intentional) risk analysis/assessment programs being conducted to evaluate any and all military materiel and personnel risks.

1. Introduction

Department of Defense (DoD) acquisition regulations require critical military programs to employ and be guided by risk management techniques that continuously assess and track the technical and programmatic/financial risks to system development and employment. [1,2,3,4,5] However, no universally adopted methodology for vulnerability risk assessment has been employed since existing techniques do not provide an adequate and reasonably supportable quantitative or qualitative basis for appropriately determining risk levels.

The purpose of this report is to describe a methodology that provides a practical and simple process for applying classical risk analysis/assessment theory to the vulnerability analysis/assessment of military systems in particular and generally to any hazard analysis desired. It applies to both weapons effects and countermeasures effects as well as to operational environment effects (natural and man-made), for the first time providing system analysts with a common/unified vulnerability assessment methodology for these diverse areas. This new vulnerability risk analysis/assessment methodology also identifies and corrects procedural errors in the traditional hazard risk analysis charts used for safety/health and many other risk assessment programs. [6]

This new methodology is applicable to all risk analysis programs conducted by the materiel development and evaluation communities and can also be used to develop initial threat and system requirements prioritizations by the combat development community. It has attributes that make it powerful in its simplicity yet thorough in its approach even for complex systems.

Hostile military threats, to include both weapons and countermeasures (CMs), are herein addressed as intentionally induced hazards to successful system operation since they are purposely imposed hostile actions designed to impair or prevent system mission accomplishment. The proposed methodology addresses and accounts for the balance between the equally important vulnerability components/factors of threat probability (likelihood of threat occurrence/encounter) and threat susceptibility (magnitude/severity of threat impact/degradation, i.e. threat effectiveness) via a "product of engagement event probabilities" approach. The methodology enables the analyst to gain a new perspective on the relative importance of these two critical components of risk when evaluating both hostile threat vulnerability risk and operational environment hazard vulnerability risk. Resultant insight gained may reveal that currently employed risk analysis processes/practices often result in the over-estimation of risk. The methodology has attributes that make it powerful in its simplicity yet thorough in its approach even for extremely complex systems, thus extending its applicability beyond system vulnerability/survivability risk assessment to a wide range of DoD and other government agency risk management programs.

A significant deficiency of current vulnerability assessment methods which employ typical "stoplight" color charts (a generic example applicable to an air defense system is shown in figure 1) is that no indication or rating procedure is given to inform the decision maker of how the vulnerability assessment level (as indicated by the color) was actually chosen, i.e. what factors were addressed, weighed, and incorporated in the determination of the vulnerability level color.

Threat	Mission	Functions			Components (HW/SW)			
	Air & Missile Defense	Sensor: Surv/Acq	Btl Mgmt: Fire Cntrl	Weapon: Engage	Radar & GSE	BMC3 & GSE	Launcher & GSE	Interceptor [In Flight]
Threat Spectrum	●	●	●	●	●	●	●	●
Threat Weapon A	●	X	X	X	●	●	●	---
Threat Weapon B	●	X	X	X	●	●	●	●
Threat Countermeasure A	●	●	●	●	X	X	---	X
Threat Countermeasure B	●	●	●	●	X	X	---	X

Figure 1. Example vulnerability assessment "stoplight" color chart.

Additionally, one is not able to tell from the chart why or how much the assessed overall vulnerability level/color might change with changes in the threat/system conditions and parameters and thus what courses of remedial action are indicated or beneficial.

Finally, no indication is given to the decision maker of the assessor's confidence in the overall vulnerability level color or in any of the contributing factors that may have been utilized. Obviously, a critical decision made based on a system vulnerability rating of High (red) and supported by a *High* confidence level might be significantly different compared to the same decision made based on a vulnerability rating of High (red) but only supported by a *Low* confidence level. Risk assessment confidence is a critical issue to decision makers and must be communicated.

1.1 Defense Suppression Threats

The basic types of threats that defense systems must address are often categorized as the offensive threat (OT, the threat(s) which the defense system is designed to defend against) and the defense suppression threat (DST, the threat techniques/tactics/devices which the enemy employs to counter the effectiveness of the defense system). Effectiveness analysis generally deals with the defense system's performance against the OT, whereas survivability analysis generally deals with the defense system's ability to survive (and, usually, operate through) intentional attacks by the DST. The system must also be designed to survive and operate through its expected operational environment extremes, both natural and man-made (both "non-intentionally" induced). An example of these threat types (in an air and missile defense system application) is shown in figure 2.

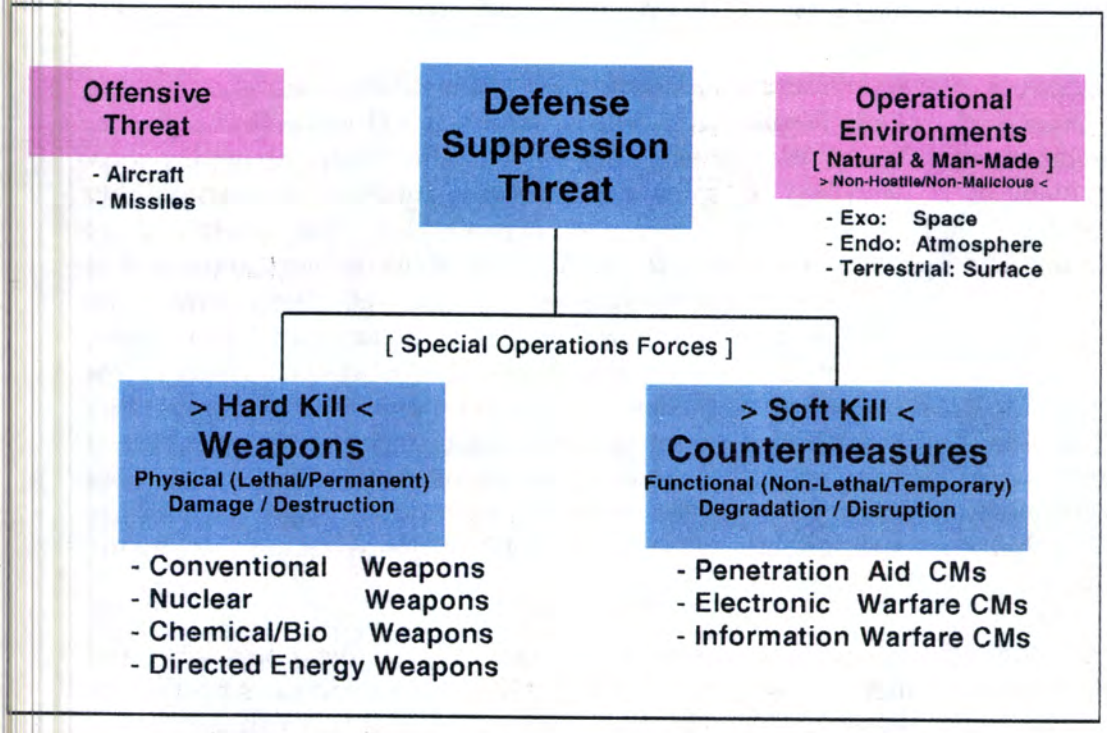

Figure 2. Threat categories for air and missile defense systems.

DSTs can be categorized as being either weapons (physical "hard kill" or permanent damage/ destruction) or countermeasures (functional "soft kill" or temporary degradation/disruption). Most DST platforms/devices are designed to deliver either one or the other in conventional operations; however, special operations forces can generally deliver either type of DST. For some DST devices, the type of kill mechanism/effect achieved depends on the circumstances/conditions (e.g., directed energy weapons can cause hard kill damage at short ranges but may only achieve soft kill degradation at long ranges).

Vulnerability assessment methodologies utilized in the past have taken completely different forms when addressing weapon effects and countermeasure effects. Weapon effects (physical destruction) vulnerability analyses and countermeasure effects (functional degradation) vulnerability analyses have suffered from the lack of a common methodology to compare their relative impact on defense system performance and effectiveness, not to mention their aggregated effects. Neither could be used to address the other, resulting in no common way to assess their relative or cumulative effects on a "level playing field". For example, silent and invisible electronic warfare (EW) countermeasures have long labored under the burden of proving their relative value/worth to aircraft survivability when compared to the immediately obvious and assessable contribution of weapons. Some of the deficiencies and shortcomings of the two current vulnerability assessment methodologies will be described first, followed by a description of a new common/unified methodology which applies equally to both.

1.2 Vulnerability Definition: Weapons [DoD Regulation 5000.2-R]

The current official definitions for survivability, vulnerability, and susceptibility are presented in DoD Regulation 5000.2-R (figure 3). These definitions were developed after World War II primarily for ballistic (weapon) applications. Survivability is described as some combinatorial function of susceptibility (openness) and vulnerability (degraded capability). The likelihood of encountering a threat, which one would logically think is very important to survivability considerations, is not addressed. These definitions provide no means to quantify any of the terms (how is "openness" quantified?) and, worse, the terms have no root connectivity to the baseline definitions given in the dictionary. It becomes confusing when one tries to rationalize how vulnerability (a bad thing) is considered a subset of survivability (a good thing). Also, if vulnerability and susceptibility are components of survivability, then does survivability quantitatively equal the product of susceptibility and vulnerability (survivability = susceptibility x vulnerability)? If not, what are the missing factors?

In dictionaries, susceptibility is generally defined as "sensitive, unresisting, and yielding to an influence/action/force" (i.e., not hard). This indicates post-attack weakness, not pre-attack openness as defined in the regulation. Also, vulnerability is generally defined as "unprotected/undefended from danger/attack; open to attack". This implies a measure of openness and exploitability, qualities attributed to susceptibility in the regulation.

Survivability:

***Survivability* is the *capability* of system and crew to *avoid or withstand* a man-made hostile environment without suffering a abortive impairment of its ability to accomplish its designated mission [*vulnerability* and *susceptibility* are components of *survivability*]**

Vulnerability:

***Vulnerability* is the *characteristic* of a system that causes it to suffer a definite degradation (loss or reduction of capability to perform its designated mission) as a result of having been subjected to a certain (defined) level of effects in an unnatural (man-made) hostile environment**

Susceptibility:

***Susceptibility* is the degree to which a weapon system is *open* to effective attack due to one or more inherent weaknesses [a function of operational tactics, countermeasures, probability of enemy fielding a threat, etc.].**

Figure 3. Vulnerability definitions: DoD Regulation 5000.2-R.

The ballistics community has traditionally defined susceptibility as essentially the probability of being hit (P_{HIT}) and vulnerability as the probability of being killed given a hit ($P_{KILL\ /\ HIT}$), which agrees semantically with neither definition. [7] Susceptibility reduction has dealt with avoiding being hit (i.e. an encounter), and vulnerability reduction has dealt with avoiding being killed, given a hit (i.e., hardness). Since the ultimate objective is to quantify survivability (where, obviously, $P_{SURVIVED} = 1 - P_{KILLED}$), what is needed here is an "ility" which is described by their product ["kill-ability (P_{KILLED})" = susceptibility (P_{HIT}) x vulnerability ($P_{KILLED\ /\ HIT}$)] but this has never been defined.

1.3 Vulnerability Definition: Countermeasures [DVAL Methodology]

Current CM vulnerability assessment methodologies also have several deficiencies. In the 1960s and 1970s, the EW vulnerability of developmental systems, which were critically dependent on the EM spectrum, was becoming an increasing concern to DoD. In 1978, the US Air Force DVAL Joint Test Force, a USDR&E/DDT, developed the current definitions of vulnerability with respect to electronic warfare (EW) CMs, called the Data Link Vulnerability Analysis (DVAL) methodology, &E chartered effort, and was approved for application by OSD in 1983. [8,9,10] The DVAL methodology was implemented via a four-phase process: (1) pre-test analysis, (2) test design, (3) test planning & execution, (4) post-test analysis. Obviously, it was based heavily on testing and test data analysis (in contrast to theoretical system analysis and vulnerability assessment) and was never universally adopted or implemented.

In 1988, the Naval Weapons Center/China Lake developed the ECCM Requirements and Assessment Manual (ERAM) via a DA-supported tri-service working group effort to study the adequacy of system ECCM requirements development and to define ORD ECCM requirements in terms of a set of ECM engagement models (ECM test design scenario descriptions). [11] The ERAM was written in a five-volume set: (1) Air-Air Missiles & Air Intercept Radars, (2) Air-Air Surveillance Systems & C3 Systems, (3) Surface-Air Weapon Systems, (4) Air-Surface Weapon Systems, and (5) Surface-Surface Weapon Systems. The ERAM also utilized the DVAL methodology EW vulnerability definitions but was basically an ECM test requirements manual, not an ECM vulnerability assessment manual.

In 1990, OSD directed the establishment of a tri-Service committee to better define the EW vulnerability assessment (EWVA) process, called the EWVA methodology. [12] It basically consisted of simply an evolution of the DVAL methodology where the interceptibility and accessibility elements were combined into a new exploitability element and a four-step process was recommended: (1) system research, (2) susceptibility analysis, (3) exploitability analysis, and (4) vulnerability analysis (to include threat assessment). It was never officially approved by OSD.

The baseline DVAL methodology describes EW vulnerability as (figure 4):

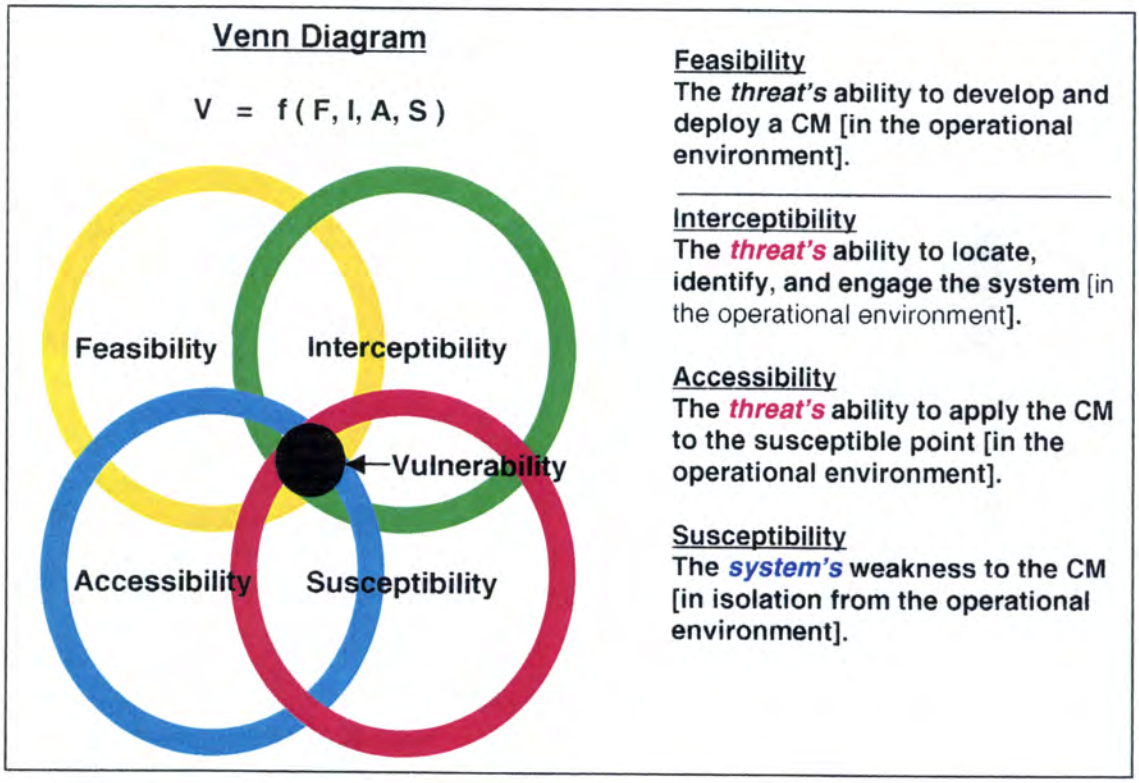

Figure 4. EW vulnerability definitions: DVAL methodology.

Vulnerabilities are the *system's* "characteristics" that cause degradation or capability reduction. These characteristics are unclear as to whether they are those of the system's components or the specific critical functions they perform. Vulnerability is further defined to be composed of four elements:

1. *Feasibility* - the *threat's* ability to develop and deploy a CM [in the operational environment]

2. *Interceptibility* - the *threat's* ability to locate, identify, and engage the system [in the operational environment]

3. *Accessibility* - the *threat's* ability to apply the CM to the susceptible point [in the operational environment]

4. *Susceptibility* - a *system's* weakness to the CM [in isolation from the operational environment]

These definitions were developed in the 1980's primarily for EW (countermeasure) applications. Vulnerability is again described as some combinatorial function of feasibility, interceptibility, accessibility, and susceptibility. Again, the likelihood of encountering a threat CM, which one would logically think is very important to survivability considerations, is not addressed. Again, these definitions provide no means to quantify, weigh, or prioritize any of the terms.

One immediately notes that the *system* vulnerability is curiously oriented toward and based upon the capabilities of the *threat* rather than on the threat resistance capabilities/characteristics of the system. If vulnerability is defined as a system characteristic, its component elements should also be defined in terms of system characteristics.

- The feasibility element (correctly defined as a characteristic of the threat) should provide a means to address more of the issues of likelihood of encounter (e.g. tactical employment/implementation feasibility) than just technical development and deployment feasibility. It also does not consider the probability of acquiring a CM capability from another source.

- The interceptibility element (defined as a characteristic of the threat) should be defined and quantified as a characteristic of the system, such as the system's inability to degrade/deny geo-location and engagement targeting by the CM. It also is not universally applicable, in particular with respect to (1) passive sensors that do not transmit signals that can be intercepted and to (2) many generic CMs (particularly passive CMs such as chaff) that do not need to locate or identify the system via the interception of some signal or signature.

- The accessibility element (defined as a characteristic of the threat) should also be defined and quantified as a characteristic of the system, such as the

system's inability to spatially/spectrally/temporally resist or reject access/penetration by the CM.

- The susceptibility element addresses only technical susceptibilities, excluding (due to the wording "in isolation from the operational environment") potential tactical/operational susceptibilities, which are due to operational or doctrinal deficiencies and limitations.

No procedure is given to determine how the elements should be combined, whether they interact as mutually exclusive or dependent probabilities, or what relative priority/weighting should be applied to each. Also, no distinction is made between "a" vulnerability/susceptibility of the system (a capability deficiency/limitation, such as inadequate jamming rejection capability) and "the" vulnerability/susceptibility of the system (the extent or probability of the deficiency/limitation). In addition, no rating criteria are given by which one might rank the relative criticality of several different vulnerabilities.

1.4 Unified Theory of Survivability: Functional and Physical

All of the above noted deficiencies in each of the individual weapon and CM vulnerability assessment methodologies are remedied by the application of a deceptively simple and universal approach to vulnerability assessment: classical risk analysis techniques. Noting that risk (inherently a probability) is classically defined as the product of the probabilities of its two critical components/factors, hazard probability/ likelihood and hazard severity/consequences, and one merely extends the concept of hazard vulnerability/risk (due to unintentional operational environment effects) to threat vulnerability/risk (due to intentional hostile actions and their effects). Letting susceptibility represent the magnitude/severity of impact/degradation (or, equivalently, the potential/probability of being severely impacted/impaired) given an encounter, consistent with the concept of weakness, the following natural result ensues:

$$P_{VULNERABLE} = P_{ENCOUNTER} \times P_{SUSCEPTIBLE}$$

and, therefore:

$$P_{SURVIVABLE} = 1 - P_{VULNERABLE}$$
$$= 1 - [\, P_{ENCOUNTER} \times P_{SUSCEPTIBLE} \,]$$

As will be shown later, all of the relevant CM vulnerability issues (feasibility, accessibility, etc) and weapon vulnerability issues (vulnerability vs. survivability) are addressed and resolved with this approach.

A significantly important by-product of this approach is the allowance of a common/ unified vulnerability assessment methodology to be utilized for both weapon and CM vulnerability assessment. This "unified theory of survivability", which allows the equivalent/uniform evaluation of *physical survivability* (vs. "hard kill" weapon effects) and *functional survivability* (vs. "soft kill" CM effects)

via a single common equation based on well-established risk analysis theory, permits the relative and comparative assessment of multiple threat effect vulnerability on a "level playing field". In fact, the concept can be taken a step further by observing that physical survivability is, in actuality, a subset of functional survivability. After all, the degradation/denial of a defense system's ability to perform its critical functions can be achieved by either temporarily disabling its critical functions (via "soft kill" CM) or by permanently destroying the critical components, which perform those functions (via "hard kill" weapons). Systems and components exist to perform functions, so functional survivability and effectiveness is the ultimate objective. Weapons and CMs merely go about denying that functionality/capability via different means and effects.

In addition, it should be noted that survivability theory is actually a subset of reliability theory and, as such, the probability mathematics associated with the reliability of parallel and series systems applies. Reliability is classically defined as the probability of being functional (i.e., acceptable functional performance under normal/natural operational environments/conditions as well as their expected extremes). Survivability addresses the probability of being functional (i.e., acceptable functional performance and operational effectiveness) despite intentional hostile attempts to degrade or deny functionality and operability.

The mechanics and details of adapting/applying traditional hazard risk analysis to threat vulnerability risk analysis, along with some of the deficiencies of those established methods, will now be discussed.

2. Hazard Risk Analysis

Risk analysis is required by regulation to be applied to all critical processes associated with the development and operation of military systems. Figure 5 presents the risk analysis chart referenced in MIL-STD-882C and used to assess health and safety hazard issues/concerns and to specify the authority responsible for verifying the resolution of any issues/concerns [13].

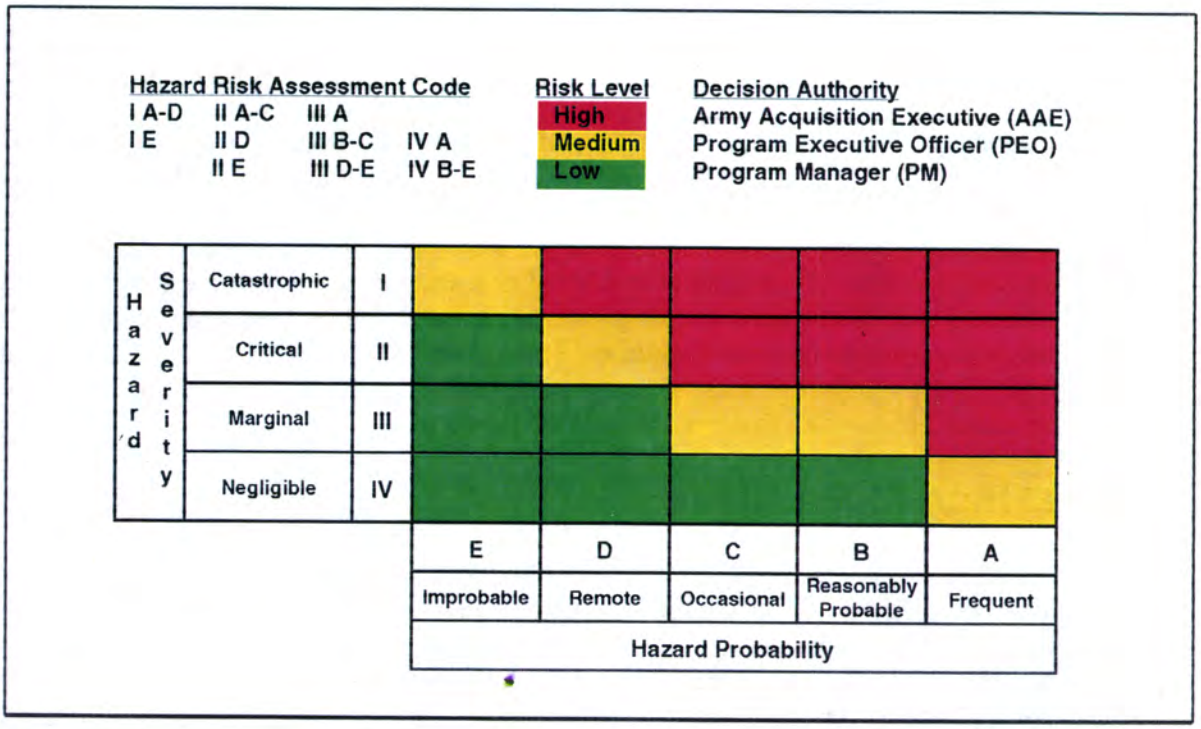

Figure 5. Health & safety hazards (MIL-STD-882C) risk matrix.

The three-level risk analysis approach addresses the two primary components, or factors, of hazard risk (hazard probability of occurrence and hazard severity of impact). It is seen that the quantification of the two component factors is made in different levels (four severity levels and five probability levels) with somewhat limited and ambiguous descriptors and no supporting numerical quantification guidance. The three categories used to describe the hazard risk level are High (red - 8 cases), Medium (yellow - 5 cases), and Low (green - 7 cases). The particular risk level assigned to the severity/probability combinations (boxes) is apparently based upon the assumption of a Medium risk level existing in the boxes composing the linear diagonal of the matrix array. It will be shown later that this assumption is unsupportable using any reasonable mathematical foundation and leads to the over-estimation of the number of High risk cases/areas.

2.1 Hazard Probability: Likelihood

The categories used to describe hazard probability (i.e., likelihood of hazard occurrence/encounter) are improbable (E), remote (D), occasional (C), reasonably probable (B), and frequent (A). No numerical quantification of any kind is provided, leaving the hazard probability component assessment open to individual interpretation of the limited and ambiguous semantic terms. The potential impact of this shortcoming on the accuracy of the ultimate risk assessment is quite obvious as the demarcation of the categories is left wide open to misinterpretation.

2.2 Hazard Severity: Impact/Consequences

The categories used to describe hazard severity (i.e., impact/consequences) are negligible (IV), marginal (III), critical (II), and catastrophic (I). No numerical quantification of any kind is provided, leaving the hazard probability component assessment open to individual interpretation of the limited and ambiguous semantic terms. The potential impact of this shortcoming on the accuracy of the ultimate risk assessment is quite obvious as the demarcation of the categories is left wide open to misinterpretation. The aggregate impact of the ambiguities of both the probability and severity component assessments on the resultant accuracy of the risk assessment is cumulatively worse.

2.3 FMECA Risk Analysis

Another risk-related analysis technique in common usage is failure mode, effects, and criticality analysis (FMECA). [14] Upon inspection of the details of the procedure as presented in MIL-STD-1629A, it becomes clear that it is in essence just classical risk analysis with the definitions changed a bit. FMECA severity is defined as the consequences of a failure mode (the potential degree of damage). This is equivalent to severity of impact as utilized in risk analysis. FMECA criticality is defined as a relative measure of the consequences (severity) of a failure mode and its frequency of occurrence. This is equivalent to risk as utilized in risk analysis, which is a measure of the severity of impact in combination with the likelihood of occurrence. Note that MIL-STD-882C on safety and health hazard risk analysis is referenced for the definitions to be used in assessing frequency of occurrence and severity. In figure 6, it is shown how the equation used to define criticality is essentially equivalent to the classical equation used to define risk, which is essentially the product of hazard effect likelihood of occurrence and effect severity of impact.

Severity: the consequences of a failure mode
[the potential degree of damage]

Criticality: a relative measure of the consequences [severity]*
[Risk] of a failure mode [due to a threat/hazard effect]
and its frequency of occurrence *

$$C = \Sigma \left(P_{\text{FAILURE EFFECT}}\ R_{\text{FAILURE RATE}}\ t_{\text{OPERATION}}\ X_{\text{\% APPL TO FAILURE MODE}}\right)_n$$

$$[\ \text{Risk} = P_{\text{EFFECT OCCURRENCE}} \times P_{\text{EFFECT SEVERITY}}\ ]$$

* MIL-STD-882C (Safety) referenced for level definitions

Figure 6. FMECA (MIL-STD-1629A) definitions.

3. Vulnerability Risk Analysis/Assessment

Hazard vulnerability can be thought of as the risk (or probability) of functional mission failure/defeat due to the effects of natural or unintentional man-made operational environment hazards. Viewing hostile threats as intentionally imposed hazards to system operability and survivability, threat vulnerability is simply the risk (i.e. probability) of functional mission failure/defeat due to the threat effects (DST weapon effects or CM effects). Equivalently, survivability is the probability of functional mission success/ accomplishment in spite of the threat effects (or other natural or unintentional man-made operational environment hazards). The probability relationship between vulnerability and survivability can be expressed as follows (figure 7):

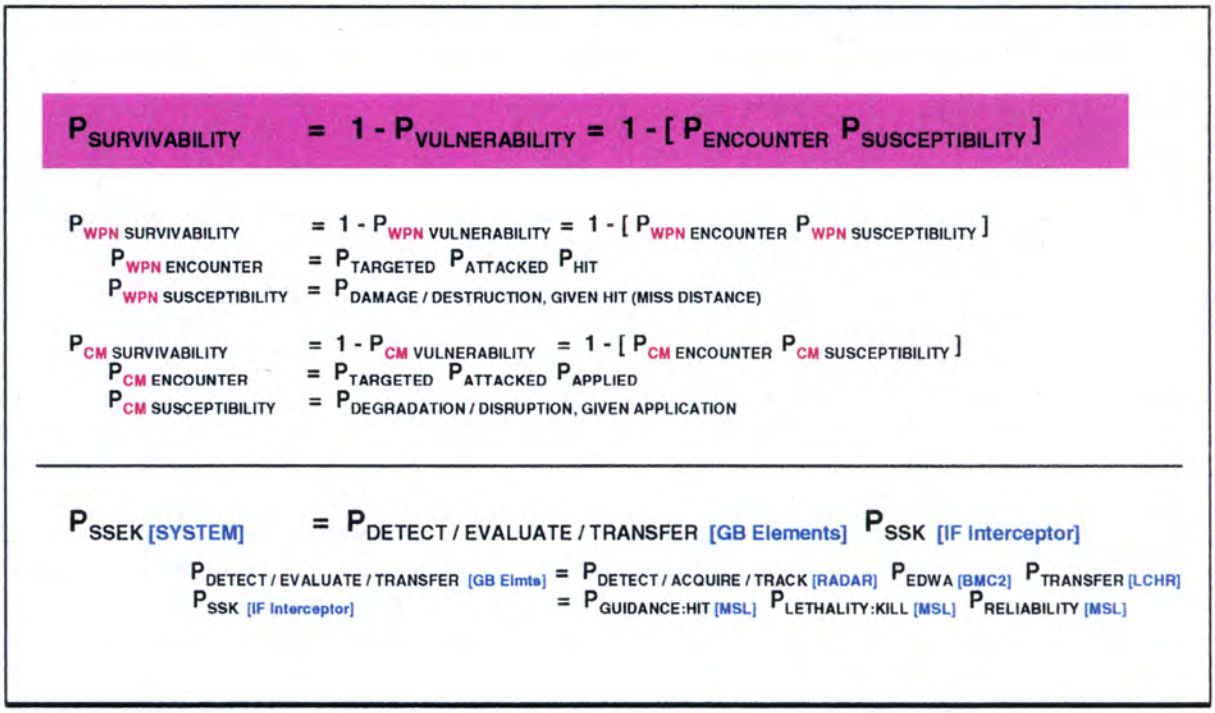

Figure 7. Vulnerability risk definitions.

$$P_{SURVIVABLE} = 1 - P_{VULNERABLE}$$
$$= 1 - [P_{ENCOUNTER} \times P_{SUSCEPTIBLE}]$$

where, for weapons effects:

$$P_{ENCOUNTER} = P_{TARGETED} \times P_{ATTACKED} \times P_{HIT}$$

$$P_{SUSCEPTIBLE} = P_{KILLED\ /\ HIT}$$

and, for CM effects:

$$P_{ENCOUNTER} = P_{TARGETED} \times P_{ATTACKED} \times P_{APPLIED}$$

$$P_{SUSCEPTIBLE} = P_{KILLED\ /\ APPLIED}$$

Note that $P_{TARGETED}$ is employed instead of the more commonly used $P_{DETECTED}$ due to the fact that, in general, much more than just target detection is required to support a target attack, to include target precision geo-location or tracking, identification/discrimination, selection/prioritization, and engagement decision and weapon assignment (EDWA) functions.

This all makes logical sense because, if a system is 95 percent vulnerable to being physically/functionally "killed" (95 percent chance/risk of functional failure ... Very High vulnerability), it obviously must be 5 percent survivable to being physically/functionally "killed" (5 percent chance/probability of functional success ... Very Low survivability). It should be emphasized here that vulnerability is hereby being defined as a stochastic/probabilistic risk (i.e., vulnerability risk) and is not a 1 or 0 (vulnerable or not vulnerable) issue as it has been so often treated in the past. Since threat vulnerability is obviously a type of system risk, it can be assessed via classical risk analysis in a similar manner as general hazard vulnerability risk. In accordance with classical risk assessment theory, the two primary components of threat vulnerability risk are therefore threat probability (likelihood of threat occurrence/encounter) and threat susceptibility (magnitude/severity of threat impact/degradation).

For weapons (whose effects are permanent "hard kill" damage/destruction), we're essentially addressing *physical survivability* (critical component kill).

For countermeasures (whose effects are temporary "soft kill" degradation/disruption), we're essentially addressing *functional survivability* (critical function kill). These definitions are in accordance with common sense, agree with the definitions in the dictionary, and are quantifiable.

It should also be noted that, to avoid confusion and potential misinterpretation of the results, one must clearly determine where $P_{ENCOUNTER}$ stops and $P_{SUSCEPTIBLE}$ starts, i.e. exactly what the targeted impact point and intended impact/effect are. A classic CM example is the stand-off jamming (SOJ) vulnerability of a radar. If one simply considers the device under attack to be the radar system, $P_{ENCOUNTER}$ addresses the likelihood of ECM signal delivery to the face of the radar antenna

and $P_{SUSCEPTIBLE}$ addresses the integrated impact of the CM effect on the response of the radar system as a whole. However, if one specifically considers the actual *functional impact point* which is the radar detector (e.g., noise jamming attempting to deny adequate signal-to-noise ratio via noise injection) or the radar data processor (e.g., deception jamming attempting to confuse true target tracking via false target injection), $P_{ENCOUNTER}$ now addresses the likelihood of ECM signal delivery/penetration to the detector which now includes the likelihood of overcoming the spatial rejection of the radar's antenna side lobes and the spectral/temporal rejection of the radar's signal processor filters/gates, whereas $P_{SUSCEPTIBLE}$ now addresses the impact of the CM effect on the response of just the radar detector (or data processor). Similarly, a weapon example would require $P_{ENCOUNTER}$ to address the likelihood of weapon delivery (ballistic, guided, deposited, etc) to the targeted *physical impact point* (i.e., a "hit" defined as an impact within the minimum miss distance required for effect deposition) and would require $P_{SUSCEPTIBLE}$ to address the impact of the weapon effect on the system functionality/operability.

A significant added benefit of defining survivability and vulnerability in probability terms (besides making common sense) is that it facilitates the incorporation of survivability analysis results into common effectiveness analyses formats (themselves derived from probability-based ORD requirements) where system bottom line effectiveness is defined in probability terms (as represented in figure 7 by air defense weapon system probability of single shot effective kill, P_{SSEK}).

In attempting to assess vulnerability risk via the utilization of the hazard risk chart described previously, the deficiencies and shortcomings of the hazard risk chart led to an investigation of the risk level definitions/derivations which in turn resulted in the redefinition/expansion of the chart to improve its utility and accuracy. The resulting modifications are described below.

Figure 8 presents an improved five-risk state/level (Very Low, Low, Medium, High, Very High) threat vulnerability risk assessment matrix to better facilitate the assessment of threat vulnerability risk as accurately as possible. Critical issues in the utility of this risk state matrix are the number of quantization levels employed for each risk component/ factor and the definition of these levels because these determinations will uniquely bound the accuracy/resolution of the resulting risk estimates. It was determined that a minimum of five quantization levels for each risk component are required to adequately assess threat vulnerability risk. This results in a 5 x 5 matrix that is partitioned into five corresponding risk states/levels denoted by the colors orange (Very High), red (High), yellow (Medium), green (Low), and blue (Very Low). The rationale for the employment of a minimum of five levels of quantization is given in the following sections.

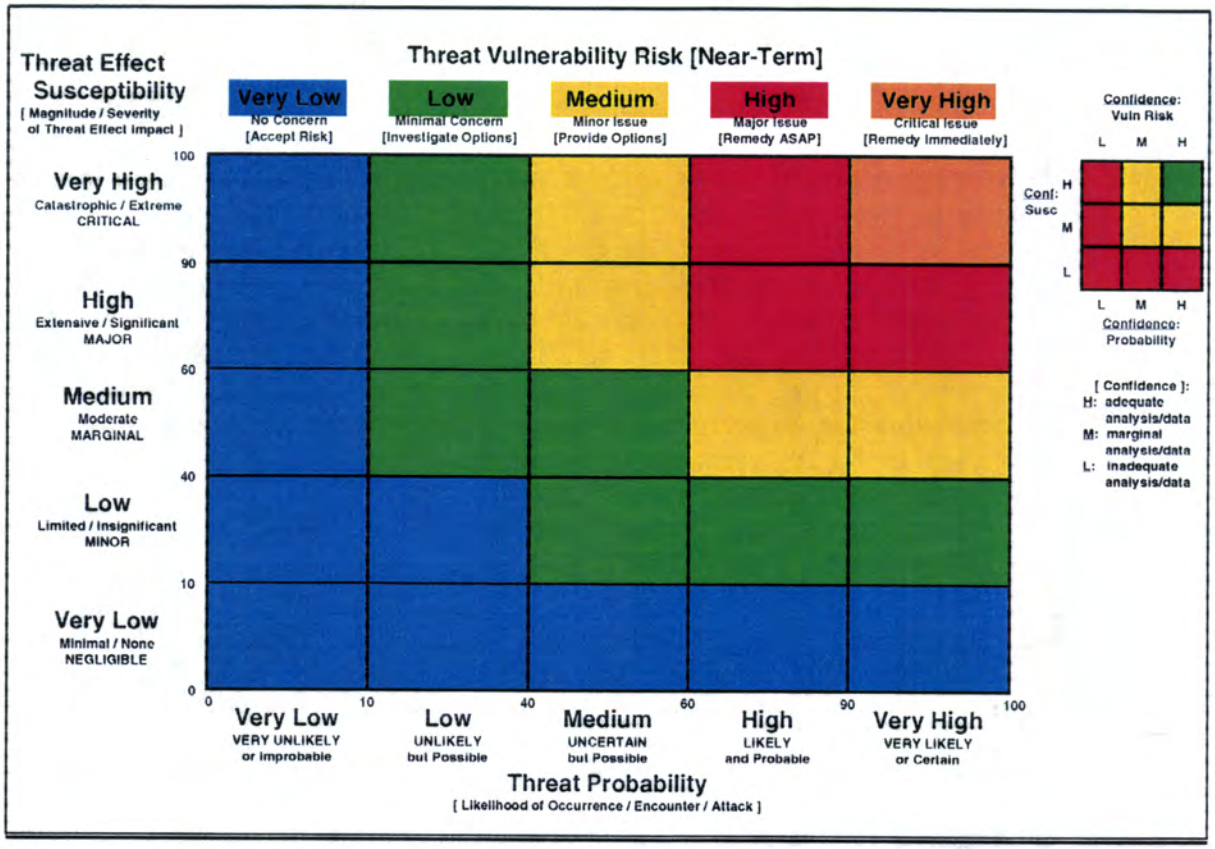

Figure 8. Vulnerability risk assessment matrix.

3.1 Threat Probability: Likelihood of Encounter

In order for threat vulnerability risk to be adequately assessed, threat probability (likelihood of occurrence/encounter/attack) should be quantizied to a minimum of five levels. Both qualitative descriptors and quantitative values are used to enhance the clarification and refinement between the quantization levels and to provide two alternative yet mutually complementary means to resolve potential differences of opinion and/or perspective. The qualitative descriptors were chosen to be specific enough to allow clear differentiation between the levels but not be so limited as to be unusable. For example, the High and Low probability categories are easily distinguished due to the obvious difference between likely and unlikely. High and Medium are distinguished due to the distinction of probable as opposed to merely possible. Medium and Low are distinguished due to the distinction of uncertain as opposed to decidedly unlikely. The quantitative values were chosen via the following rationale: a 10 percent range for both Very High and Very Low is widely accepted as reasonable in many threat assessment documents [15]; a ± 10 percent range provides a sufficient yet not excessive range of uncertainty surrounding a 50/50 chance (and generally it

is desirable to limit, as much as possible, the amount/extent of the range of unknowns/uncertainties); the remaining 30 percent ranges for both High and Low are the natural result. These are nominal values that should suffice under most situations, but can be negotiable based upon the specific application (a purely probabilistic approach might favor "equally divisible" intervals such as a ± 12.5 percent range around the 50/50 point and a 12.5 percent range for Very High and Very Low). It is recommended that these levels be adopted as a general standard to permit universal applicability and comparative correlate-ability. A prudent and rational application of this methodology will verify that risk level determinations should not be significantly sensitive to minor changes in the component level quantizations. Any resulting instances of risk level ambiguity/disagreement should not be frequent enough to cause appreciable concern.

System threat assessment reports (STARs) have generally assessed reactive threats in accordance with a minimal two level approach: "most likely" or "technologically feasible". "Most likely" does not specify how likely; a critical issue in risk analysis because all of the "most likely" threats could potentially be, in actuality, unlikely. "Technologically feasible" does not specify likelihood at all, is often just assumed to mean unlikely, and does not specifically address tactical/operational feasibility. These categories are open to broad interpretation when used to support the determination of threat vulnerability risk because they do not give an adequate indication of threat probability. It is recommended that threat probability be mandated to be quantified into the five minimum quantization levels described.

Threat probability assessment is not a trivial task and requires significant intelligence community resources and analysis capabilities. Because expertise and experience in system threat response analysis and vulnerability analysis is not necessarily available in the intelligence community, the vulnerability analysis community must provide assistance in the assessment of the many relevant issues. Threat probability assessments must be performed for both existing (baseline) and projected (reactive) threats. They must address, as a minimum, the following threat acquisition/development difficulty (technical likelihood) issues:

- system design/operation knowledge required and available/accessible,
- threat design/operation knowledge/skills required and available/accessible,
- threat technology required and available/accessible,
- threat test/simulation/verification capability required and available/accessible,
- threat manufacturing/production capability required and available/accessible, and
- cost effectiveness (economic affordability).

They must also address, as a minimum, the following threat employment/ implementation difficulty (tactical likelihood) issues:

- time frame: near-term, mid-term, far-term;
- country: state of technological maturity and operational capability;
- location: region, area, geography (or battle space tier);
- situation/circumstances/conditions: climate/weather, reconnaissance/surveillance/target acquisition (RSTA), offensive/defensive posture;
- attack coordination/timing and logistics requirements;
- criticality/value/success/effectiveness perceptions and expectations;
- desired objectives and intended impact (psychological factors);
- military/operational execution practicality/viability/applicability (to include detrimental effects of threats on basic system operation/effectiveness); and
- cost effectiveness (economic affordability).

3.2 Threat Susceptibility: Severity of Impact

In order for threat vulnerability risk to be adequately assessed, threat susceptibility should be quantizied to a minimum of five levels. Both qualitative descriptors and quantitative values are used to enhance the clarification and refinement between the quantization levels and to provide two alternative yet mutually complementary means to resolve potential differences of opinion and/or perspective. The qualitative descriptors were chosen to be specific enough to allow clear differentiation between the levels but not be so limited as to be unusable and were chosen via the same rationale described previously. For example, the High and Low severity of impact categories are easily distinguished due to the obvious difference between major/extensive and minor/limited. High and Medium are distinguished due to the distinction of significant as opposed to merely marginal. Medium and Low are distinguished due to the distinction of marginal as opposed to decidedly insignificant. The quantitative values were chosen via the following rationale: a 10 percent range for both Very High and Very Low is widely accepted as reasonable in accordance with the same rationale used for threat probability; a ± 10 percent range provides a sufficient yet not excessive range of uncertainty surrounding a 50/50 choice (and generally it is desirable to limit, as much as possible, the amount/extent of the range of unknowns/uncertainties); the remaining 30 percent ranges for both High and Low are the natural result. These are nominal values that should suffice under most situations, but can be negotiable based upon the specific application (a purely probabilistic approach might favor "equally divisible" intervals such as a ± 12.5 percent range around the 50/50 point and a 12.5 percent range for Very High and Very Low). It is recommended that these levels be adopted as a general standard to permit universal applicability and comparative correlate-ability. A prudent and rational application of this methodology will verify that risk level determinations should not be significantly sensitive to minor changes in the component level quantizations. Any resulting

instances of risk level ambiguity/disagreement should not be frequent enough to cause appreciable concern.

The underlying system functional performance response analyses, which support the threat susceptibility assessment, are accomplished via classical system analysis techniques and are verified/validated via simulation/test data. The qualitative descriptor denoting the severity of impact, based on the predicted or demonstrated potential for system degradation or impairment, is then selected.

3.3 Threat Vulnerability Risk

An assessment is defined as a judgment (an expert opinion) that is made based upon expertise and experience, supported by available quantitative/qualitative analyses and verifying/validating information and data. As such, the inherent associated approximations, vagarities, and general perceptions involved in making an assessment must be kept in mind. Attempts toward excessive rationalization, without supporting analysis or data, should be avoided since a judgment is still subject to interpretation. However, differences in opinion between analysts/assessors should be manageable for a five-state/level risk quantization. For example, if two analysts disagree over whether the resultant risk is major (High) or minor (Medium), the problem may lie in the component factor assessments and should be resolved at that lower level with greater ease.

In order for threat vulnerability risk to be adequately assessed, it should be quantized to a minimum of five states/levels. Figure 9 shows that, when employing linear scales for both axes, the risk bands representing the five risk states/levels are not linear across the matrix array diagonal as is assumed in figure 5. When the two component probabilities are multiplied, the resulting vulnerability risk probability bands are hyperbolic and symmetric around the diagonal connecting the upper right (1/1) and lower left (0/0) points. The resulting symmetrical shape is also independent of the number of quantization levels. Figure 9 also shows that linear risk bands do result if a log scale is used for both axes, but log scales have never been specified as the intended measure for the risk components.

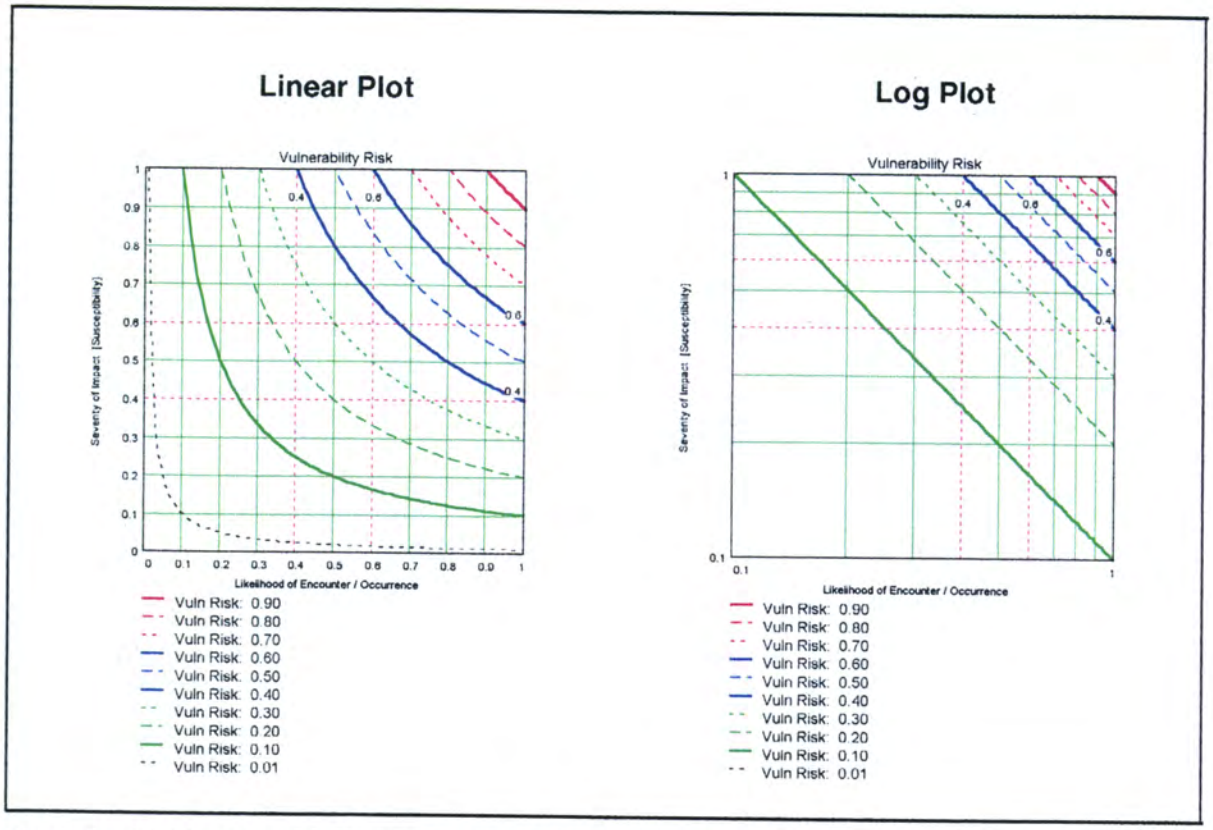

Figure 9. Risk bands with linear and log plots.

This can be seen clearly when the two risk components are each quantized to ten equal levels (which is not realistically practical for threat vulnerability risk analysis or any other risk analysis) resulting in the 10 x 10 matrix of figure 10. The criteria used for determining the risk rating for each case (determining the associated color for each box) assumes that the whole box takes on the risk level of the highest rated point in the box. The ranges chosen for the quantization levels of each risk component determine the thickness/extent of the risk bands.

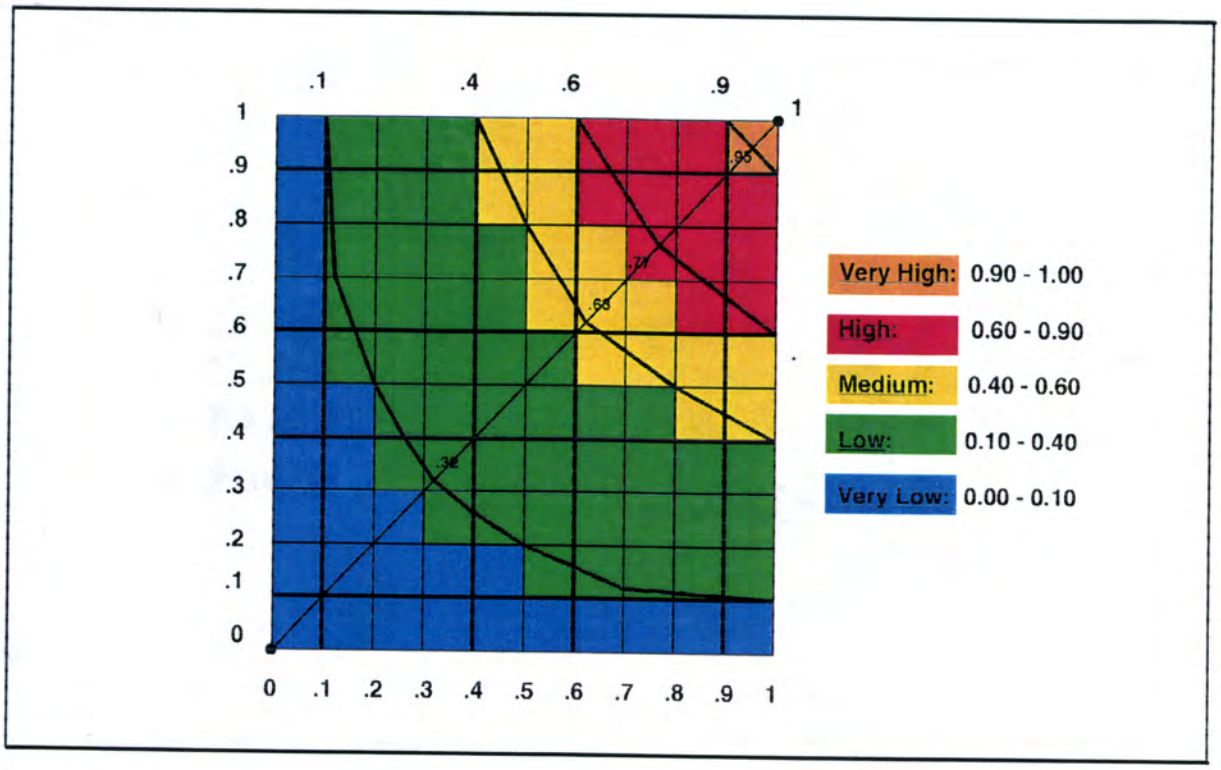

Figure 10. Ten-by-ten quantization of component probabilities.

At first inspection, the risk bands may appear to be circles around the 1/1-point. However, when the two components are infinitesimally quantized as was shown in figure 9, the risk bands are seen to be hyperbolics. Useful insight into actual risk levels is gained in applying this modified chart to risk assessment. A significant decrease in the occurrence of Very High and High-risk cases is seen to result in comparison with figure 5. There is potential for wide ranging implications resulting from this reduction in the number of major and critical risk cases indicated and the associated cost of remedying them in the many areas within DoD and other government agencies where risk assessment is utilized.

Converting the 100-position (10 x 10) matrix into a 25-position (5 x 5) matrix with the recommended five-quantization levels for each component and using equal-size intervals results in figure 11. This is actually a more accurate representation of figure 8 when taking actual quantization range scaling into account. The equal area boxes of figure 8 are required to facilitate annotation during implementation, however one should keep in mind that the actual relative sizes of the boxes are as shown in figure 11.

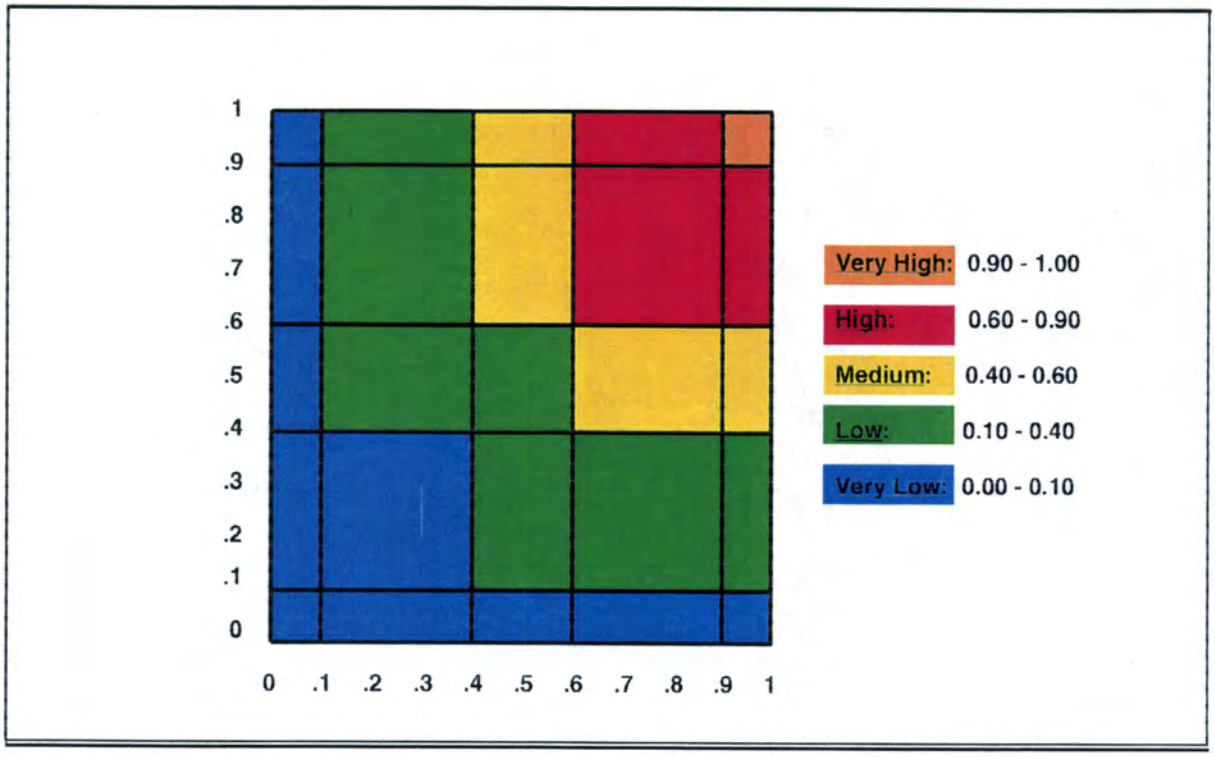

Figure 11. Five-by-five quantization of component probabilities.

The importance of the likelihood of encounter factor in determining vulnerability risk cannot be stressed too heavily. Susceptibilities are essentially exploitable weaknesses. Vulnerability (which actually tells us whether the susceptibility is an immediate concern, that is, something we really need to "worry about" and remedy in the near term) must include the important measure of the likelihood of encounter/occurrence. For example, the human body has a Very High susceptibility (exploitable weakness) to bullets. If hit, there is a very high likelihood that serious damage to the body will occur. So why is it that we don't walk around wearing bulletproof vests or even worrying much about this susceptibility? The reason is that, in reality, we instinctively know that our vulnerability is Very Low ... because the actual daily likelihood of being shot (encountering bullets) is very low. Thus the bottom line factor which influences/drives our primary (and logical) response to this severe threat is seen to be not our very high susceptibility to bullets but our very low vulnerability to bullets.

Additional insight into the importance of threat likelihood may also be gained when considering the security classification of susceptibilities and vulnerabilities. For example, the Jul 98 National Missile Defense (NMD) security classification guide (SCG) defines the following:

- *system level vulnerability*: classified Top Secret (TS)
- *element level vulnerability*: classified Secret (S)
- *TS vulnerability*: an exploitable weakness [i.e. susceptibility] that would render the *system* inoperable [i.e., ineffective] and result in a single point failure.
- *S vulnerability*: a weakness at the *element* level, which will <u>not</u> render the system inoperable and does <u>not</u> result in a single point failure. However, it has the following contradictory classification statements:
  - A system level vulnerability is classified TS *until "mitigation" of the weakness is complete.*
  - If a solution (which "eliminates" the weakness) *is being implemented [i.e. not complete]*, then the vulnerability can be classified S.

Traditionally, vulnerabilities have been classified as TS when they have been demonstrated/ verified/proven and classified as S when they have been merely predicted/indicated/ suggested via analysis/simulation/testing.

Applying a few common sense rules with respect to the actual and immediate severity of impact of a known susceptibility/vulnerability on the security/defense of our interests or forces can aid in the determination of meaningful security classifications:

- *System in development*: A known* susceptibility/vulnerability, which is in the process of being remedied ("mitigation" must be complete by IOC), should be S because enemy knowledge of it *cannot be immediately* exploited/used to defeat the system (cause mission failure) in combat operations [this more specifically conforms to the implied intention of (6)]
- *System in deployment*: A known* susceptibility/vulnerability, even if in the process of being remedied ("mitigated"), should be TS because enemy knowledge of it *can be immediately* exploited/used to defeat the system (cause mission failure) in combat operations [this more specifically conforms to the implied intention of (5)]

---

*Known means proven and verified via test and demonstration, not just projected/predicted via analysis or simulation.

The bottom line with regard to the security classification of vulnerability is as follows:

- threat projected/predicted => should be classified *S*
- threat known + system in development => should be classified *S*
- threat known + system in deployment => should be classified *TS*

Often, for analytical purposes, it is desirable to plot the vulnerability risk (or, equivalently, the survivability probability) in terms of its component factors as continuously variables. For example (figure 12), if a threat "effect X" has a likelihood of encounter of Medium ($P_{ENCOUNTER}$ range of 0.40 to 0.60) and a system susceptibility (severity of impact) of High ($P_{SUSCEPTIBILITY}$ range of 0.60 to 0.90), then the resulting $P_{SURVIVABILITY}$ is seen to range from Medium (1 - [0.60 x 0.90] = 0.46) to High (1 - [0.40 x 0.60] = 0.76). Should one be able to determine $P_{ENCOUNTER}$ and $P_{SUSCEPTIBILITY}$ to a greater level of accuracy, a corresponding greater level of accuracy for $P_{SURVIVABILITY}$ can be achieved. A chart such as this can aid the analyst in determining the driving factors behind a system's $P_{VULNERABILITY}$ and thus indicate whether it would be more beneficial to ameliorate the vulnerability by attempting to lower the threat $P_{ENCOUNTER}$ via measures which decrease threat targeting, attack, and hit capabilities or by attempting to lower the system $P_{SUSCEPTIBILITY}$ via measures which increase system resistance or hardness to the effect.

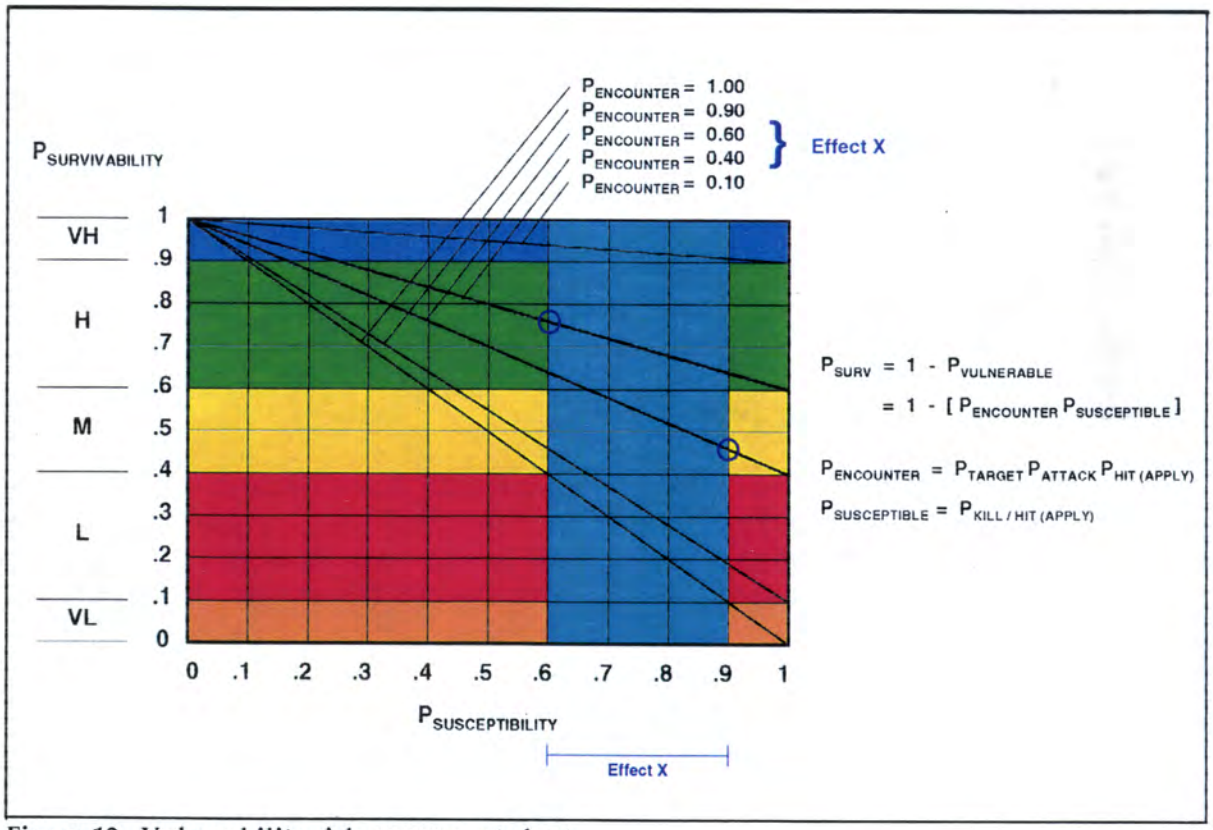

Figure 12. Vulnerability risk assessment chart.

3.4 Sensitivity Analysis: Threat Parameter Variations

This methodology can be used to address another critical problem in vulnerability risk analysis: the determination of threat vulnerability risk sensitivity to threat parameter variations. This can be accomplished by expanding the "system versus threat" analysis to a greater level of detail and assessing "critical subsystems/components/functions versus specific threat parameters" issues. Individual threat parameters and threat parameter sets/combinations can be analyzed/evaluated as to their probability of occurrence and severity of impact on each of the system's critical components and functions. The results tend to support the general premise that threat parameters/sets that produce greater impact are often less likely to be encountered due the greater power requirements, greater technical or operational difficulty/complexity, or greater expense and will therefore generally tend to remain in or close to the same risk band as the parameters jointly vary. For example, infrared (IR) sensor system performance impact versus flares increases with the flare ejection rate, but the actual impact on the system's vulnerability risk is correspondingly offset by the decreased likelihood/difficulty of carrying the number of flares necessary to provide protection over extended areas and periods of time. Radar system performance impact versus cross-polarization electronic countermeasures (ECM) increases with the accuracy of cross-polarization achieved, but the actual impact on the system's vulnerability risk is correspondingly offset by the likelihood/difficulty of achieving the exact parametric accuracy necessary under operational conditions.

Applying the methodology this way also provides an audit trail or means of tracking the risk status versus time as system changes and threat changes occur. The risk assessment matrix permits one to visually follow and monitor changes in the corresponding risk components and the resultant system threat vulnerability risk rating as a function of time as reactive threat capabilities and likelihoods increase and system capabilities increase as system modifications and improvements are added.

It must be emphasized here that all risk assessments are good for only a single point in time since both the threat probability and the system susceptibility vary with time due to enemy threat capability changes and system design modifications/changes. Risk assessments should be provided for key points in the system's operational life cycle such as the system development/acquisition milestones, initial operational capability (IOC), and at regular intervals thereafter.

Figure 13 provides a hypothetical example of the general application and proper use of this threat vulnerability risk assessment methodology and, additionally, portrays its use to evaluate system vulnerability risk sensitivity to threat parameter variations. The example utilized is the case of infrared (IR) flare decoy CMs employed against an air defense system interceptor that utilizes an IR

seeker. The air defense system's critical subsystem/component/function chart on the right shows that the IR flares are applicable to (i.e., potentially effective against, and therefore requiring analysis) the missile element (specifically, the IR seeker) but are not applicable to the radio frequency (RF) radar element or to the RF battle management/command/control/communications (BMC3) element. It also indicates what missile/seeker critical functions may be effected and the nature of the effects: (1) acquisition: false target deception, (2) track: disruption, and (3) guidance/hit: miss distance degradation.

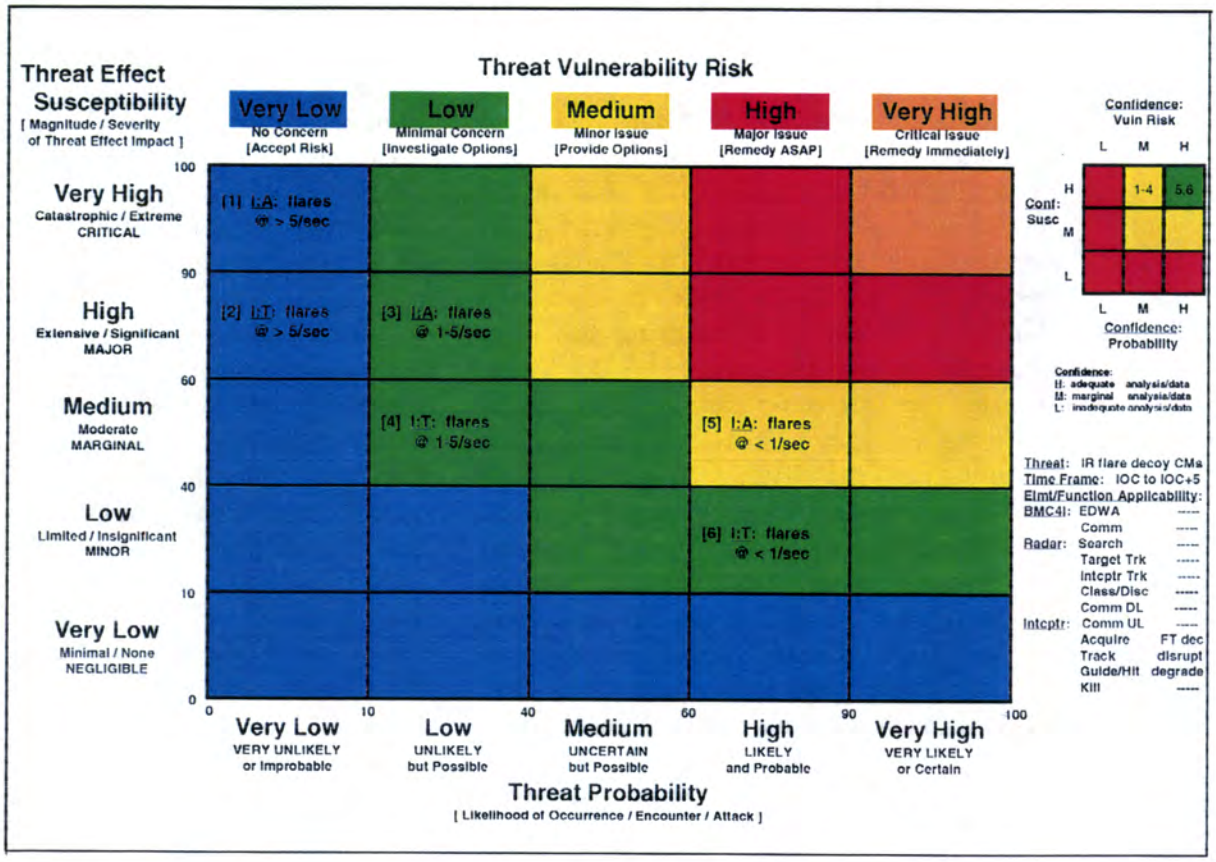

Figure 13. Example: IR flare vulnerability parametric sensitivity.

Figure 13 demonstrates how varying the CM parameter of flare dispensing rate can effect the CM vulnerability risk of the system as a combined function of the expected/ demonstrated impact on system functional performance (CM susceptibility) and the likelihood that a particular dispensing rate (or range of dispensing rates) will be encountered (CM probability). As shown here, flare dispensing rates of greater than five flares per second are rated as very unlikely to be encountered because at that rate the target aircraft could not carry enough flares to provide protection for any length of time (assuming that the aircraft does not have a missile warning receiver to alert the aircraft to a missile

approach and enable flare conservation via dispenser optimization). Flare dispensing rates of greater than five flares per second are rated as having (1) a *critical* impact on the interceptor acquisition function (denoted as I:A) because at that rate the seeker could not possibly acquire the target due to the false target deception caused by the flare decoys, and (2) a *major* impact on the interceptor tracking function (denoted as I:T) because at that rate the seeker would have great difficulty tracking the target and rejecting the disruptive effects of the flares. The resulting CM vulnerability risk is seen to be *very low* due to the influence/domination of the CM probability factor. Even though a flare-dispensing rate of greater than five flares per second has a *high* to *very high* CM effectiveness/susceptibility, the actual risk to the system is negligible because such high rates will practically never be encountered. Similar arguments apply to the other flare dispensing rates under consideration. The overall result is that, in this hypothetical example, only the impact of flare dispensing rates of less than one flare per second on the acquisition function is of concern (medium risk). If flare rates of one to five flares per second become more probable than currently rated (more probable than "unlikely"), the acquisition function risk increases to *medium* due to its *high* susceptibility to these rates. As system improvements are added (decreasing the CM effectiveness at these rates) and responsive threat dispensing rate capabilities increase (increasing the CM probability at these rates), one can track and project the cumulative/ combinatorial effects on the overall vulnerability risk to the system.

The confidence in the risk determination for each of the above cases is given to serve as a guide to the reliability of the results. For case (1), assessed to be a *very low* risk, the confidence in this risk assessment is only *moderate* (as denoted in the confidence chart at top right). This is due to the fact that, although the confidence in the CM susceptibility rating is high, the confidence in the CM probability rating is only moderate (i.e., it is uncertain that flare rates of greater than five per second are really "improbable").

It is easy to see how the vulnerability risk of the system (in this case, an IR seeker) can be tracked versus time as system modifications lower its CM susceptibility and as threat advances raise the threat likelihood of encounter, providing the decision maker a user-friendly visual audit trail of vulnerability risk versus the evaluation timeframe.

3.5 Integrated Threat Spectrum Analysis: Multiple Threat Attacks and Synergistic Threat Effects

The vulnerability risk methodology has another significant attribute in that it provides a simple straight-forward way to determine the aggregate probability of system survivability to the integrated threat spectrum ($P_{\text{SURVIVABILITY: THREAT SPECTRUM}}$) where multiple threat attacks with cumulative and/or synergistic threat effects need to be analyzed (figure 14).

The five general attack/engagement cases that need to be addressed in survivability analyses are:

1. single threat attacks: effects applied
2. multiple threat attacks (sequential): effects not cumulative/synergistic
3. multiple threat attacks (sequential): effects cumulative/synergistic
4. multiple threats attacks (simultaneous): effects not cumulative/synergistic
5. (multiple threats attacks (simultaneous): effects cumulative/synergistic

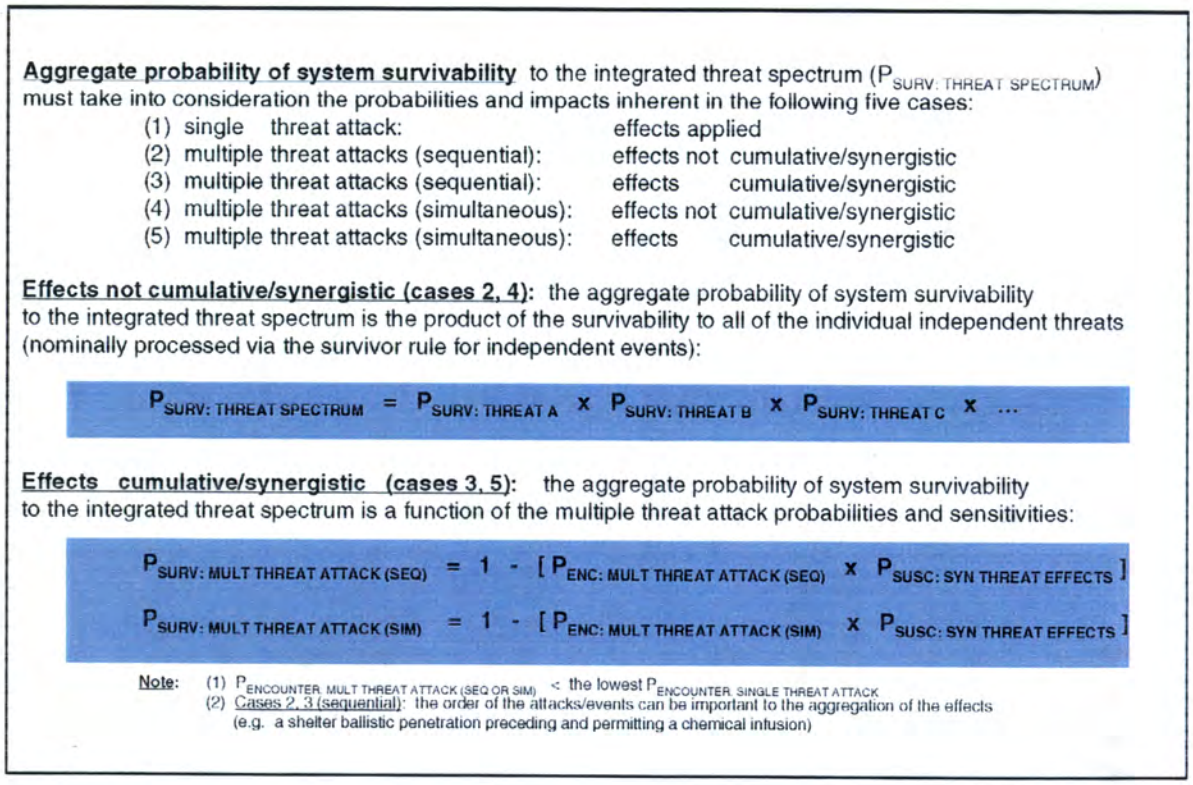

Figure 14. Integrated threat spectrum analysis.

For the cases in which the individual threat effects are not cumulative or synergistic (cases 2 and 4), the aggregate probability of system survivability to the integrated threat spectrum is simply the product of the survivability to all of the independent individual threats (nominally processed via the survivor rule for independent events):

$$P_{\text{SURVIVABILITY: THREAT SPECTRUM}} = P_{\text{SURV: THREAT A}} \times P_{\text{SURV: THREAT B}} \times P_{\text{SURV: THREAT C}} \times \ldots$$

For the cases in which the individual threat effects are cumulative and/or synergistic (cases 3 and 5), the aggregate probability of system survivability to the integrated threat spectrum is a function of the multiple threat attack (sequential or simultaneous) probabilities and sensitivities determined via application of the vulnerability risk methodology:

$$P_{\text{SURVIVABILITY: MULTIPLE THREAT ATTACK (SEQUENTIAL)}} = 1 - [\, P_{\text{ENCOUNTER: MULTIPLE THREAT ATTACK (SEQUENTIAL)}} \times P_{\text{SUSCEPTIBLE: SYNERGISTIC THREAT EFFECTS}} \,]$$

and

$$P_{\text{SURVIVABILITY: MULTIPLE THREAT ATTACK (SIMULTANEOUS)}} = 1 - [\, P_{\text{ENCOUNTER: MULTIPLE THREAT ATTACK (SIMULTANEOUS)}} \times P_{\text{SUSCEPTIBLE: SYNERGISTIC THREAT EFFECTS}} \,]$$

It should be noted that $P_{\text{ENCOUNTER}}$ for a multiple sequential threat attack and for a multiple simultaneous threat attack is obviously less than the lowest $P_{\text{ENCOUNTER}}$ for any of the individual component single threat attacks. Also, for cases 2 and 3 (multiple sequential threat attacks), the sequential order of the attacks/events can be important to the aggregation of the effects. For example, a shelter attack by conventional weapons (resulting in ballistic penetration/perforation) which precedes an attack by chemical weapons (resulting in subsequent chemical infusion) would most likely have a significantly different result than if the chemical attack preceded the conventional weapon attack. The likelihood of encounter of each individual sequence/order must therefore be addressed separately.

In figure 15, a generic vulnerability risk assessment matrix depicts how the common vulnerability presentation of all integrated threat spectrum elements (weapons, countermeasures, and operational environments) would appear. One can visually assess the relative impact of "hard kill" and "soft kill" effects on system survivability quickly and easily from a common vantage point.

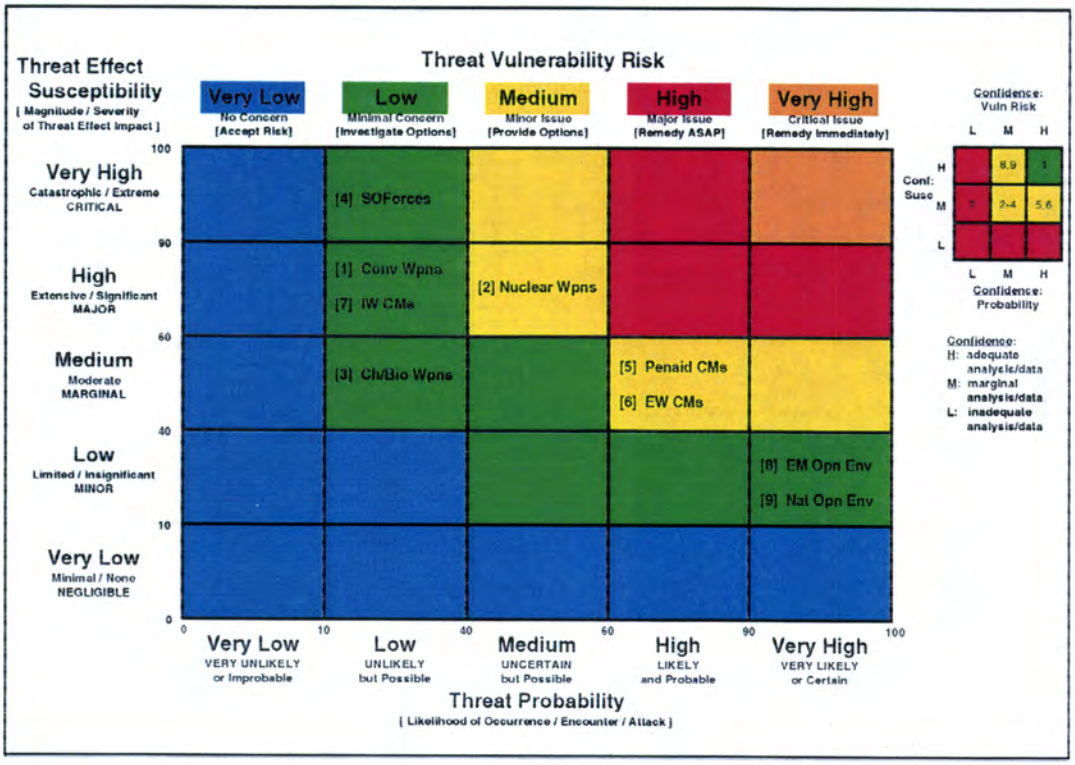

Figure 15. Integrated threat spectrum vulnerability risk matrix.

3.6 Threat Probability: STAR Fidelity Requirements

Current STAR threat assessments address two major threat categories: (1) the system-specific threat, and (2) the reactive threat. The system specific threat (consisting of both IOC and IOC+10 threats) is further broken down into suppression of enemy air defense (SEAD) threats and other threats. The reactive threat (consisting of both tactics/doctrine and technology) is further broken down into likely threats (often with unspecified dates, i.e. IOC+?) and technologically feasible threats (often with no determination of their likelihood as well as unspecified dates).

Also, STARs have generally assessed reactive threats in accordance with a minimal two level approach: "most likely" or "technologically feasible". "Most likely" does not specify how likely; a critical issue in risk analysis because all of the "most likely" threats could potentially be, in actuality, unlikely. "Technologically feasible" does not specify likelihood at all, is often just assumed to mean unlikely, and does not specifically address tactical/operational feasibility. These categories are open to broad interpretation when used to support the determination of threat vulnerability risk because they do not give an adequate indication of threat probability.

A more understandable (system specific) threat categorization would be (1) the baseline threat (i.e., existing/projected for IOC) and (2) the reactive threat (i.e., projected for IOC+X). But even more important is the need for a quantification of the threat likelihood to the five state levels described previously so that employment in the vulnerability risk assessment methodology would be facilitated. Some current threat documents (e.g., the NMD STAR) do quantify certain threats (e.g., penetration aids) to this level for the various applicable timeframes but do not quantify all of the relevant threats to this requisite detail. [15] Quantifying all threats to the five state level would allow for an equitable and equivalent assessment of system vulnerability risk across the entire threat spectrum and thus result in a greatly improved and much more useful and balanced assessment for decision makers.

3.7 System Analysis Process Structure

We are now able to visualize how the vulnerability risk assessment methodology logically fits into the overall system survivability analysis process (**figure 16**). Note here that personnel or soldier survivability (SSv) analysis can be performed via the same methodology since the soldier is just another (often, the most critical) component of the system.

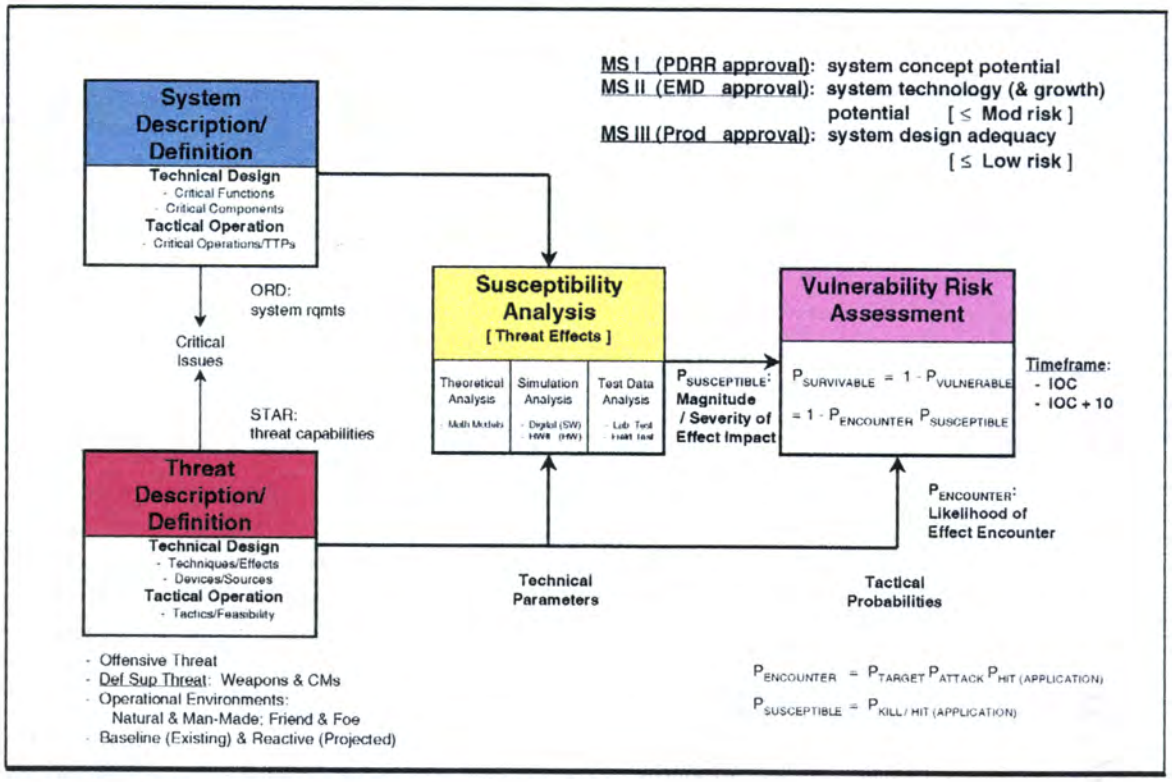

Figure 16. System analysis process.

First, the *susceptibility* analysis to determine $P_{SUSCEPTIBLE}$, the potential magnitude/ severity of impact of the threat effect(s), is conducted by theoretical analysis, simulation analysis, and/or test data analysis. This evaluation basically addresses the sensitivity of the system design parameters to the DST (and to operational environment hazards, if desired) technical parameters. Second, the *vulnerability risk* analysis is conducted to assess $P_{VULNERABLE}$ by factoring in $P_{ENCOUNTER}$, the likelihood of occurrence/encounter of the threat/environmental effect(s), which takes into account the threat tactical probabilities associated with the particular timeframe of interest (IOC, IOC+10, etc). The importance of the probability of actually encountering a particular threat/hazard, as required by classical risk analysis (not to mention common sense), is obviously emphasized so that system survivability and/or soldier survivability is not unduly overestimated by overemphasis of susceptibilities/weaknesses.

4. Vulnerability Risk Confidence

A risk assessment is incomplete, and probably even misleading to decision makers, without some form of accompanying confidence rating to indicate the status of the underlying assumptions and the adequacy of the supporting analyses/simulations/tests used to make the assessment. A significant deficiency of current vulnerability assessment methods (and "stoplight" color charts in particular) is that no confidence rating indication or rating procedure is given to inform decision makers of the risk assessment confidence, adequacy, or status. As is well known in classical defense system effectiveness analysis, system effectiveness and the confidence level in that effectiveness value are completely different and independent things, and both are essential to describe and evaluate a system. Effectiveness is a property of the system and analysis/simulation/testing is used to determine that value. Confidence level describes probabilistically how well the effectiveness value is known as a result of the analysis/simulation/testing extensiveness. Thus a system effectiveness of 70 percent (the actual, unchanging value) may only be known/proven with a confidence level of 80 percent based on limited testing but may later be known/proven to a confidence level of 95 percent with more extensive testing. Note that there is no connection between the invariant effectiveness value and the variable confidence numbers.

The 3 x 3 confidence rating matrix in the upper right corner of figure 8 (used in tandem with the risk matrix itself) remedies this deficiency in a manner that is straightforward and easy to understand. For each vulnerability risk assessment performed on each threat/hazard parameter set or combination, the evaluator's confidence in the resultant threat vulnerability risk rating is presented as a function of his confidence in each of the respective risk component ratings (threat probability and threat susceptibility). For the threat susceptibility confidence rating, the quantity and quality of the system performance analysis and/or system performance data available is considered and evaluated/judged by the assessor as to its adequacy for reaching a susceptibility conclusion. The resultant high, medium, or low confidence indication should be adequate to give decision makers a relative general indication of the status and adequacy of the system susceptibility assessment. For the threat probability confidence rating, the quantity and quality (fidelity) of the threat projection analysis and/or data available is considered and evaluated/judged by the assessor as to its adequacy for reaching a likelihood of encounter conclusion. The resultant high, medium, or low confidence indication should be adequate to give decision makers a relative general indication of the status and adequacy of the threat probability assessment. The resultant overall confidence in the vulnerability risk assessment determination is simply the intersection of the confidence judgments for the component factors as indicated in the 3 x 3 confidence rating matrix. A quick glance at the 3 x 3 matrix will indicate whether any of the vulnerability risk assessments in the risk matrix chart are not of high confidence and perhaps suspect or in need of further investigation.

One should keep in mind that these confidence determinations can often be subjective and may not always be based or upon objective numerical data or statistical calculations, as is the case with statistical confidence level/interval assessments. The confidence determinations can often be merely a statement of the assessor's judgment of the adequacy and accuracy of the analyses and data supporting the risk assessment. However, as mentioned previously, it is easy to see how a vulnerability risk assessment of high (red) which is accompanied by a high (green) confidence rating and the same assessment accompanied by a low (red) confidence indication could have totally different meanings to a decision maker faced with an important decision.

There are numerous sources of system and threat (and operational environment) parameter uncertainty/error involved in the quantification accuracy of susceptibilities and encounter likelihood. Generally, the uncertainties consist of two types: (1) random (precision error), quantities which vary from trial-to-trial that have an inherent irreducible distribution of occurrence, and (2) systematic (bias error), quantities which do not vary from trial-to-trial or engagement-to-engagement that could be reduced to precise values (or eliminated) if they were known but are represented by a range of likely values. Therefore the vulnerability risk assessment methodology actually involves the use of a Bayesian analytical framework to model both random and systematic uncertainties with probability density functions (pdf). Depending on the type of variable modeled, the pdf used to model the uncertainty associated with the parameter either (1) can indicate likelihood or frequency of occurrence based on actual data (i.e. characterization of actual empirical data) or (2) can be judgmental (i.e. based upon expert opinion). The Bayesian probabilistic approach is both mathematically rigorous (due to its technical soundness) and flexible (due to the provision of convenient mathematical models). The methodology is also flexible enough to permit the evaluation of the sensitivity of the results to various system and threat parameter variations. The methodology therefore is not necessarily a rigid black box calculation with a specific output but rather a flexible method for obtaining general results and trends.

For susceptibility analysis, we are concerned with estimating the probability of failure (unacceptable impact/stress on functional performance or physical survivability) in accordance with the following criteria

$$P_{FAILURE} = P\,(\text{Stress} > \text{Threshold})$$

where Stress represents the available functional degradation or component damage values and Threshold represents the corresponding required values that result in failure. There are significant uncertainties in the many system and threat factors that drive the Stress and Threshold values. Under the Bayesian framework of probability, both Stress and Threshold are modeled as random variables and defined by pdfs. $P_{FAILURE}$ can therefore be calculated by

$$P_{FAILURE} = \int_0^{\infty} f_{STRESS}(x,\bar{\mu})\, F_{THRESHOLD}(x,\bar{\sigma})\, dx$$

where $f_{STRESS}(x,\bar{\mu})$ and $f_{THRESHOLD}(x,\bar{\sigma})$ are the pdf for Stress and Threshold [$\bar{\mu}$ and $\bar{\sigma}$ are vectors defining the appropriate parameters, e.g. mean, standard deviation, etc] and $F_{THRESHOLD}(x,\bar{\sigma})$ is the cumulative distribution function (cdf) of $f_{THRESHOLD}(x,\bar{\sigma})$

$$F_{THRESHOLD}(x,\bar{\sigma}) = \int_{-\infty}^{\infty} f_{THRESHOLD}\ (x,\bar{\sigma})\, dx$$

Since both Stress and Threshold are random variables, $P_{FAILURE}$ is also a random variable with an associated pdf. With the exception of a few simple pdf forms (e.g., uniform, Gaussian, exponential) for $f_{STRESS}(x,\bar{\mu})$ and $f_{THRESHOLD}\ (x,\bar{\sigma})$, an explicit closed form expression for the pdf of $P_{FAILURE}$ is difficult to obtain and therefore the use of numerical techniques are generally more practical to compute the pdf.

Given that a frequency of occurrence distribution or pdf for $P_{FAILURE}$, $f_{FAILURE}(P_{FAILURE})$ [or a cdf for $P_{FAILURE}$, $F_{FAILURE}(P_{FAILURE})$, from which the pdf can be derived] can be estimated, and then Bayesian confidence bounds can be calculated. [Note that the spread (standard deviation) in the pdf is due to systematic uncertainties. If no systematic uncertainties existed, $f_{FAILURE}(P_{FAILURE})$ would be a Dirac delta function located at the expected value of $f_{FAILURE}(P_{FAILURE})$.] For example, a one-sided Bayesian confidence bound for $P_{FAILURE}$ can be computed via the following:

$$C = 1 - \int_0^{p_{FAIL}} f_{FAILURE}(P_{FAILURE})\, dP_{FAILURE}$$

where C is the desired confidence bound and p_{FAIL} is the chosen value of $P_{FAILURE}$. Typical Bayesian confidence bounds for a notional set of results are presented in figure 17. The Low, Medium, and High distribution variances result in various confidence levels as a function of the expected $P_{FAILURE}$. For example (in the notional example), the confidence (cumulative $P_{FAILURE}$, $F_{FAILURE}$) that the mean value of p_{FAIL} is less than 0.50 is 80 percent for the medium $P_{FAILURE}$ ($f_{FAILURE}$) pdf variance shown. Note that, as the amount of systematic uncertainty is reduced, the "S" curves will converge. Thus the estimation of confidence levels and bounds is highly dependent on the uncertainties that have been incorporated (or not incorporated) into the parameter models.

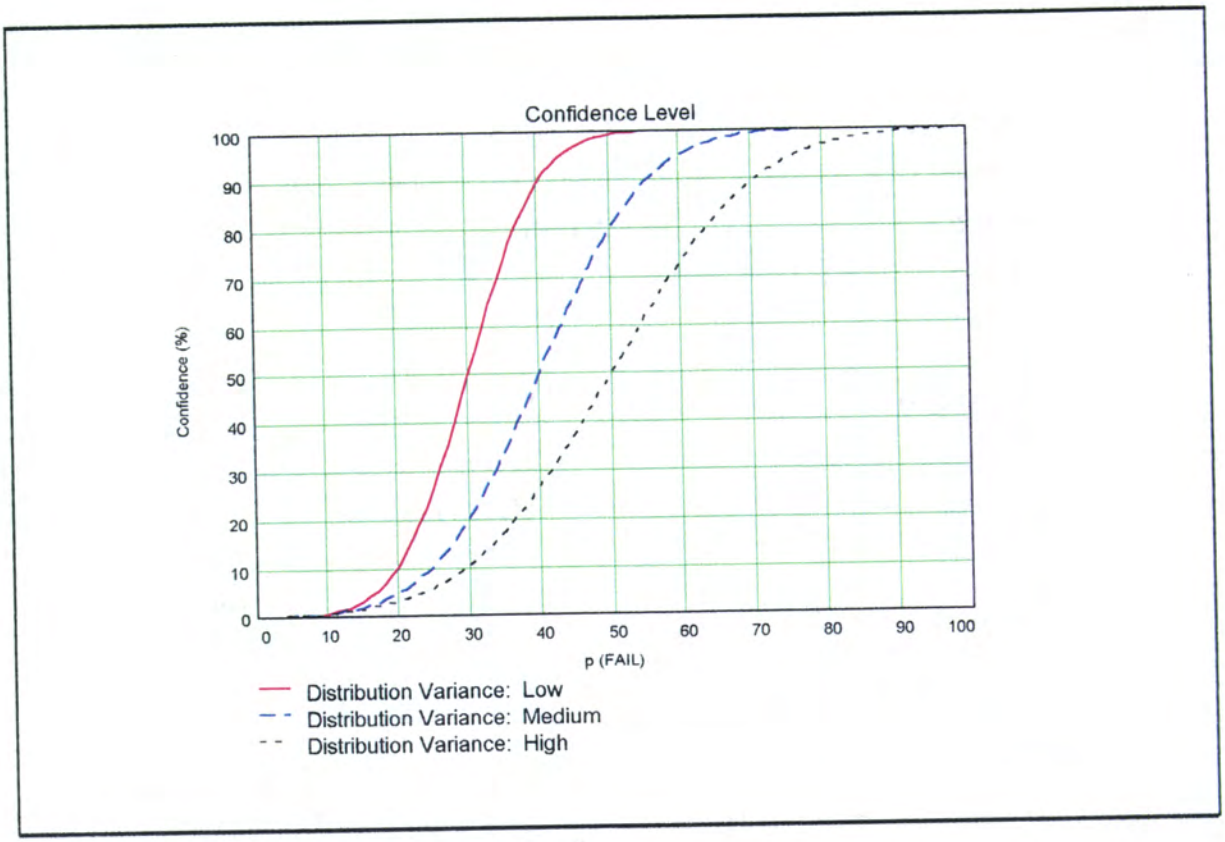

Figure 17. Typical Bayesian confidence bounds.

The actual application of the above expressions to specific cases involves the proper (or convenient) definition of the pdfs of the numerous uncertainty/error sources incorporated in $f_{STRESS}(x,\bar{\mu})$, $f_{THRESHOLD}(x,\bar{\sigma})$, and thus $P_{FAILURE}$.

5. Vulnerability Risk Tolerance

A point of confusion often arises in risk assessments relative to the applicability or relation of risk tolerance to the risk assessment results. The not-so-obvious answer is that the assessed risk level, which is a "cold, hard, calculated" value, is independent of the risk tolerance (the acceptability that risk level) and is not changed by it (figure 18).

Risk level (color): independent of (not impacted by) **risk tolerance**
- **evaluator**: responsible for **risk level** assessment
  => cold, hard, calculated engineering number
- **decision maker**: responsible for **risk tolerance** determination
  => value judgments involved [emotion, perception, beliefs]
  (vs cost, time, feasibility, priorities, alternative options)

==> a low **risk tolerance** does NOT retroactively change the **risk level**
[e.g.: child car seats, nuclear war]

Conclusions: must specify **risk level** and nominal risk mgmt responses
[Low: accept risk Med: address risk High: remedy risk]

Recommendations: may suggest mitigation of **risk tolerance**

Risk confidence: independent of (does not impact) assessed **risk level (color)**
[dependent only on adequate/sufficient analysis/data]

==> a low **risk confidence** does NOT change the **risk level (color)**

Figure 18. Risk tolerance.

For example, an evaluator's assessment of the risk of a child being injured or killed in an auto accident will likely result in a very low risk based upon the proportion of times children are involved in accidents (let alone injured/killed) relative to the number of times children are transported in cars. However, the large number of child car seats that are sold attests to the fact that many people (the decision makers) are unwilling to accept/tolerate the risk despite how low it is. Another example is that the vulnerability risk to nuclear war, to which there obviously is a very high (catastrophic) susceptibility, is low based primarily upon the fact that it has a low likelihood of occurrence (supported by the fact

that it has not occurred in the past 50 years) but the amount of money spent on nuclear deterrence and defense again attests to our extreme intolerance to that low risk. But that intolerance does not retroactively change the fact that our vulnerability risk to nuclear war is actually low, despite how incongruous that may seem.

The bottom line is that a low risk tolerance does not (retroactively) change an assessed low risk level to a higher risk level. The evaluator is responsible for an accurate, impartial risk level assessment; the decision maker is responsible for any subsequent risk tolerance determinations. Report conclusions should provide the assessed risk level and may also provide the generic/nominal risk management responses usually associated with those levels (i.e., the nominal response to low risk is usually to accept the risk whereas the nominal response to high risk is usually to remedy the problem), although the actual response taken is up to the decision maker based on his assigned risk tolerance. The issue of risk tolerance is not in the purview of the evaluator and should not be included in the conclusions, but suggestions may be made in subsequent recommendations.

An additional note here (if not already obvious from previous discussions) is that the vulnerability risk level assessed is also independent of its confidence rating and is not changed by it. The bottom line here is that a low risk confidence does not recursively/retroactively change an assessed low risk level to a higher risk level.

6. Application to Lethality Analysis: Kill Effectiveness

Another significant benefit of the vulnerability risk assessment methodology is its natural applicability to lethality analysis (or, more accurately, kill effectiveness analysis). This becomes obvious when one realizes that friendly system vulnerability (the probability of being functionally or physically "killed" by the enemy system) is equivalent to enemy system kill effectiveness (the probability of "killing" the friendly system) and vice versa. Hard/soft kill effectiveness (P_{SSK}) is simply the product of $P_{HIT\ (APPLICATON)}$ (hard kill weapon hit/delivery capability or soft kill CM application capability) and $P_{KILL\ /\ HIT\ (APPLICATION)}$ (weapon hard kill lethality or CM soft kill lethality). The applicable kill effectiveness analysis matrix is presented in figure 19. $P_{HIT\ (APPLICATION)}$ in kill effectiveness is the functional equivalent of $P_{ENCOUNTER}$ in vulnerability risk since the likelihood of encountering a weapon/CM effect is equivalent to the opponent's capability to deliver/apply it. $P_{KILL\ /\ HIT\ (APPLICATION)}$ in kill effectiveness is the functional equivalent of $P_{SUSCEPTIBLE}$ in vulnerability risk since the magnitude/severity of impact (susceptibility) to a weapon/CM effect is equivalent to an opponent's capability to achieve a kill given a hit/application (lethality).

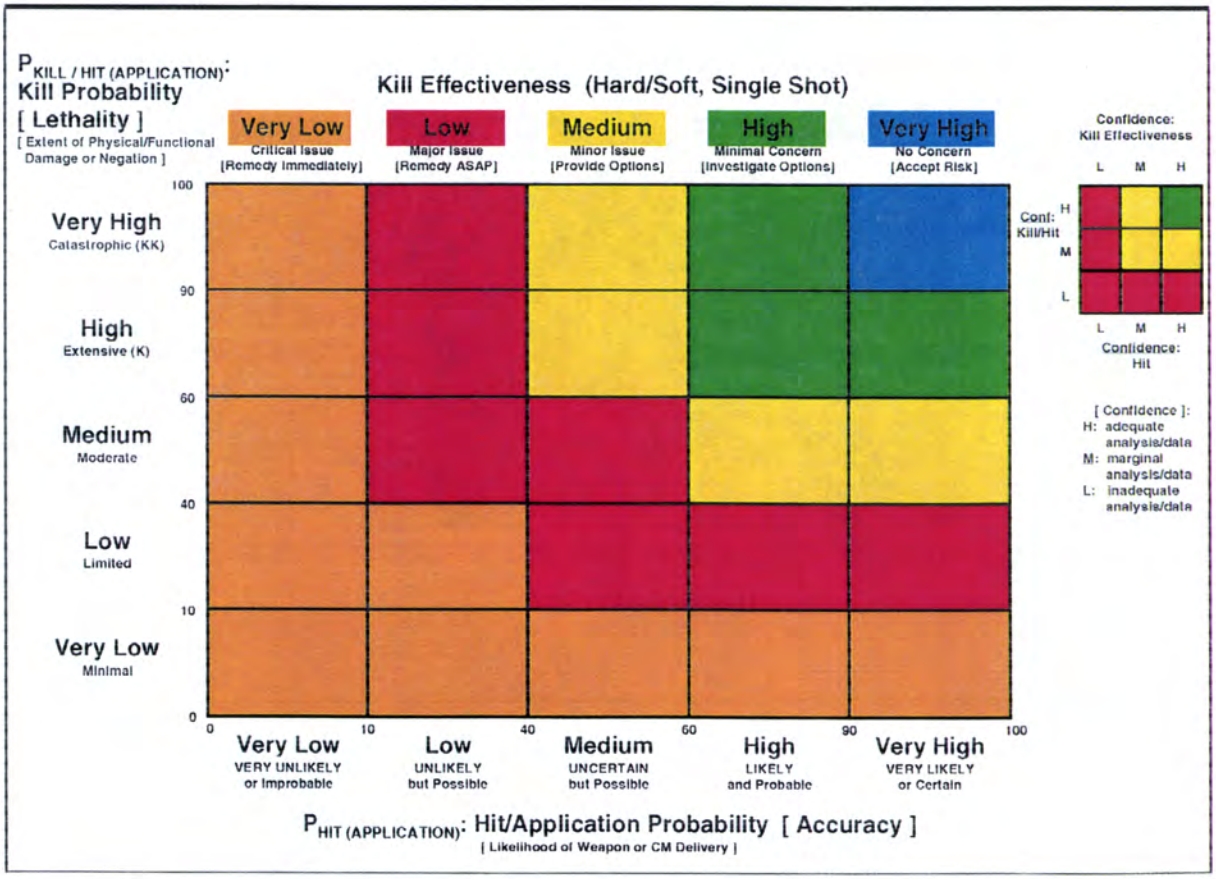

Figure 19. Kill effectiveness analysis matrix.

Often, for analytical purposes, it is desirable to plot the kill effectiveness in terms of its component factors as continuously variables just as was done for vulnerability risk.

For example (figure 20), if a "target A" has a probability of weapon hit or CM delivery/application of High ($P_{HIT\ (APPLICATION)}$ range of 0.75 to 0.90) and a probability of hard or soft kill (lethality) of High ($P_{KILL/HIT}$ range of 0.75 to 0.90), then the resulting kill effectiveness P_{SSK} [often denoted as P_{SSEK}] is seen to range from Medium (0.75 x 0.75 = 0.56) to High (0.90 x 0.90 = 0.81). Should one be able to determine $P_{HIT\ (APPLICATION)}$ and $P_{KILL\ /\ HIT\ (APPLICATION)}$ to a greater level of accuracy, a corresponding greater level of accuracy for P_{SSEK} can be achieved. A chart such as this can aid the analyst in determining the driving factors behind a system's P_{SSK} and thus indicate whether it would be more beneficial to augment the kill effectiveness by attempting to increase the weapon/CM $P_{HIT\ (APPLICATION)}$ via measures which increase weapon/CM targeting, attack, and hit/application capabilities or by attempting to increase the weapon/CM $P_{KILL\ /\ HIT\ (APPLICATION)}$ via measures which overcome target resistance or hardness to the effect.

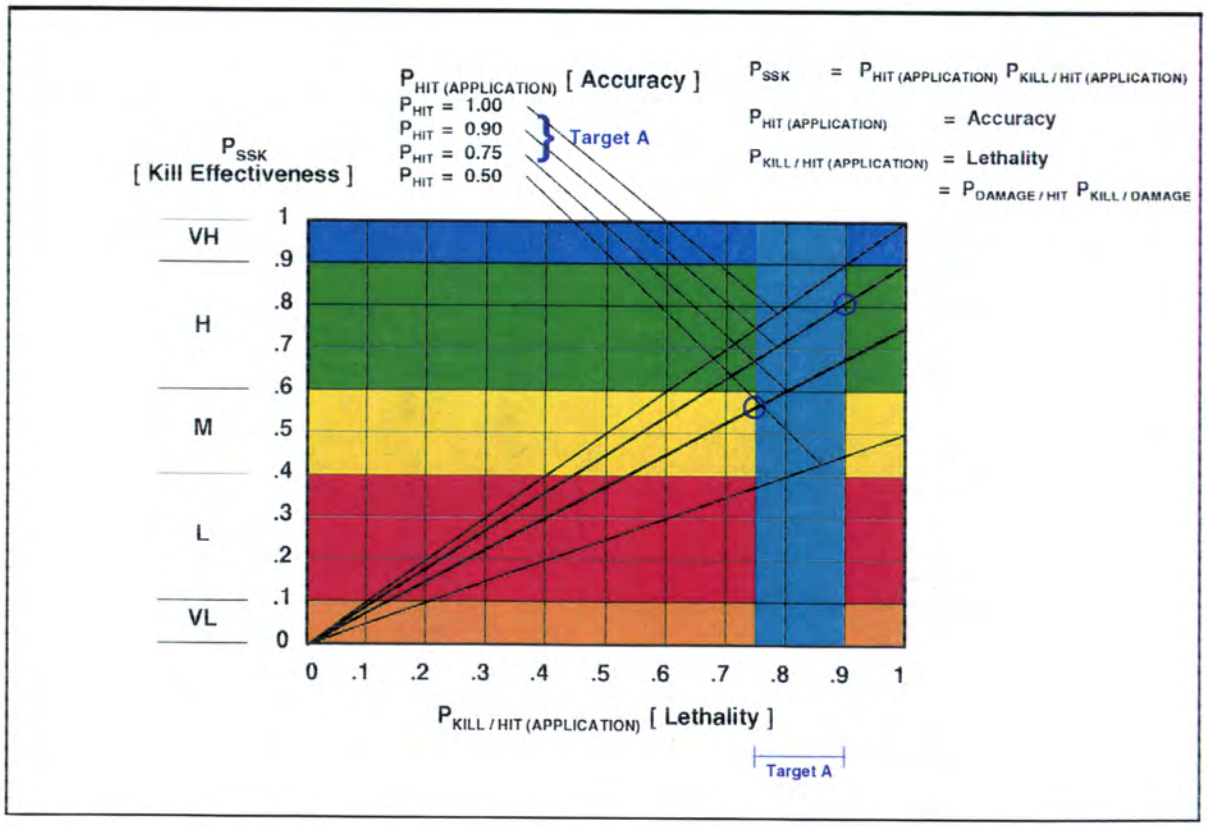

Figure 20. Kill effectiveness analysis chart.

7. Application to Effectiveness Analysis: Risk Dimensionality

The vulnerability risk assessment methodology presented provides a means to assess system (and soldier) survivability via the application of classical risk analysis techniques and procedures. The vulnerability risk analysis matrix (modeled after the hazard risk analysis matrix employed in safety and health risk analyses) employs a two-dimensional (2D) 5 x 5 matrix to evaluate the combinatorial influence of two probabilities, likelihood of threat effect encounter ($P_{ENCOUNTER}$) and potential severity of threat effect impact ($P_{SUSCEPTIBLE}$). Vulnerability risk (and hazard risk) analyzed in this manner has therefore occasionally been described as a "2D risk" but it should be noted that, by definition, risk is not two-dimensional but is instead the product of two factors describing (1) an event likelihood and (2) an event impact/consequence.

However, in everyday parlance, the term "risk" is commonly used to denote or refer to just the probability of occurrence factor since events considered "risky" are already assumed to be of high impact/consequence (e.g., dangerous events). On the other hand, effectiveness analyses conducted by the test and evaluation community often evaluate "risk" (figure 21) from the point of view of just severity of impact (the ability to meet requirements) with the assumption already made that the likelihood of the "event" (having to perform its mission) is certain. In both of these examples, the "risk" assessed is essentially addressed as a one-dimensional (1D) entity with the second risk factor just automatically assumed to be certain. In general, however, nothing is ever truly certain and should not be assumed so.

This suggests the potential use of the 2D risk matrix developed primarily for survivability (and lethality) analyses for the conduct of effectiveness analyses. One would evaluate not only the ability of a system (or a critical component) to perform a critical function but the likelihood of actually having to perform that critical function. This would give a truer indication of the actual risk to that particular function. [As an example, the vulnerability risk (or effectiveness risk) of vehicle tires to bullet damage/destruction could be addressed with the risk sensitivity chart by analyzing the likelihood of being engaged by a certain caliber of ammunition (taking into consideration the probability of round encounter as a function of range), the impact of a hit (tire damage as a function of round accuracy), and other key criteria.] As a bonus, this would unify all types of performance analyses via a common risk-based approach supported by an easy-to-use common visual presentation means and a common confidence assessment scheme. In addition, as stated previously, it would be applicable not only to analyses spanning all threat/hazard effects and issues but to all system architecture levels (from the individual subsystem/system level to the system-of-systems or family-of-systems level). It would also ensure that any "risk" analyses conducted were truly done via accepted dual factor risk analysis techniques without omitting any one of the two equally important classical risk analysis components.

Low
All components/subsystems and associated software have been developed
and are not based on any new technologies.
All subsystems and associated software have been integrated into a complete system,
and some successful testing has been done.
Analysis, simulation, and testing have demonstrated
a high probability that the requirements can be met.

Medium
Majority of components/subsystems and associated software have been developed
and undeveloped components are not based on new technologies.
The major subsystems and associated software have been integrated,
and some successful testing has been done.
Based on analysis, simulation, and/or testing, it is judged that
the requirements can be met.

Medium High
Majority of components/subsystems and associated software have not been developed.
Components have not been integrated into subsystems or have not been field tested.
Based on analysis, simulation, or testing, it is judged that there is
a marginal likelihood that the requirements can be met.

High
Technology has not been developed or has not been demonstrated outside the laboratory.
Components/subsystems or associated software have demonstrated,
based on analysis, simulation, or testing, that
the requirements cannot be met.

Figure 21. Test and evaluation community risk definitions.

Vulnerability risk due to the effects of natural and man-made operational environments and hazards (e.g., electromagnetic environmental effects, E3, and climatic/weather effects) can also be more effectively assessed via this methodology. For example, the vulnerability of radars to lightning strikes (considered part of both the E3 and weather domains) can be assessed with the risk sensitivity chart to analyze the risk based on the likelihood of encountering near-strike effects, the impact of direct strikes, and other key criteria.

Risk analysis timeframe is another important consideration. With battlefield DSTs, the likelihood of encounter of (exploitation by) a threat is normally assessed during a relatively short timeframe (a battle or an operation) and, given a kill by the threat, you are considered dead "forever" (repair or replacement is usually not considered over short periods). With natural environments/hazards, the short-term impact (damage/destruction) of severe events is obviously Very High, i.e. the system elements have Very High susceptibility. However, the likelihood of encounter/occurrence of severe natural disasters over short timeframes (like a period of heightened tensions or an actual attack) is Very Low, so the overall vulnerability risk is Very Low during short timeframes. [The likelihood of encounter/occurrence of an attack immediately after a natural

disaster (and up until repair/replacement) would probably also be Low since we would be at a heightened state of readiness/alert ... and threats usually consider this a poor time to attack.] The likelihood of occurrence of severe natural events over long timeframes (decades) is Very High and therefore the *long-term* vulnerability risk to natural disasters is Very High, but the associated *short-term* vulnerability risk to attack/exploitation after any natural disaster remains Low for the reasons given. The bottom line here is that the timeframe assessed needs to be made clear, and is especially important when dealing with infrequent natural disasters.

8. Conclusions

The new vulnerability risk assessment methodology provides a means to assess the *vulnerability risk* of systems/subsystems and their associated critical functions and critical components (to include the soldiers who operate the systems) to all survivability/operability threat categories and to all operational environment hazards (natural and man-made) as well as numerous other benefits (figure 22). It also supports and justifies the results more clearly and provides a means for indicating the assessor's *confidence* in the results. Its applicability encompasses all known hazard risk assessment categories and serves to aid the requirements development process as well as the requirements conformance evaluation process. Its applicability also extends to integrated threat spectrum considerations and the evaluation of multiple threat attacks and synergistic threat effects as well as to the related fields of lethality (kill effectiveness) analysis and performance/effectiveness analysis.

Vulnerability risk due to man-made *lethal physical "hard kill"* weapon threats (such as conventional, nuclear, and chemical/biological weapons ... to include friendly fratricide as well as hostile attack) and due to *non-lethal functional "soft kill"* CM threats (such as penetration aid CMs, electronic warfare [EW] CMs, and information warfare [IW] CMs) can be more effectively assessed via this methodology. Soldier survivability (SSv) in hostile threat environments is also more effectively assessed via this methodology than with the set of questions given in current SSV parameter assessment lists. The vulnerability risk assessment methodology developed and presented provides a simple and effective process to address these critical areas. It provides not only a more robust and accurate improved methodology for the conduct of classical risk assessments but also an associated top-level confidence assessment procedure.

Issues associated with materiel development and evaluations have been specifically addressed. However, combat developers like the Army Training and Doctrine Command to develop future materiel and doctrinal requirements could also apply this vulnerability risk assessment technique. Preliminary prioritizations of vulnerability risks associated with system survivability/operability threats or soldier survivability/operability threats (including operational environment hazards) could be developed. No clear method has been previously available to the combat development community to develop and evaluate system requirements based on the principles of risk analysis. With this methodology, future requirements determinations can be better substantiated and subsequent determinations of whether operational requirements have been met by the materiel developers can be better supported.

An important result of this risk analysis methodology is that the actual number of High and Very High risk cases assessed will be significantly reduced with respect to that obtained by utilizing current (health and safety hazard) risk analysis charts. Applying this methodology could thus impact the amount of time and funding expended on unnecessary system "gold plating" to meet hostile

threat and/or operational environment hazard cases currently inaccurately assessed as being High or Very High risk.

This methodology also provides an audit trail allowing the tracking of risk status as a function of time as system changes and threat changes occur. Its ability to allow the determination of vulnerability risk assessment *sensitivity to threat parameter variations* is a critical attribute that augments the evaluation community's capability to project realistic and reasonable threat vulnerability risk.

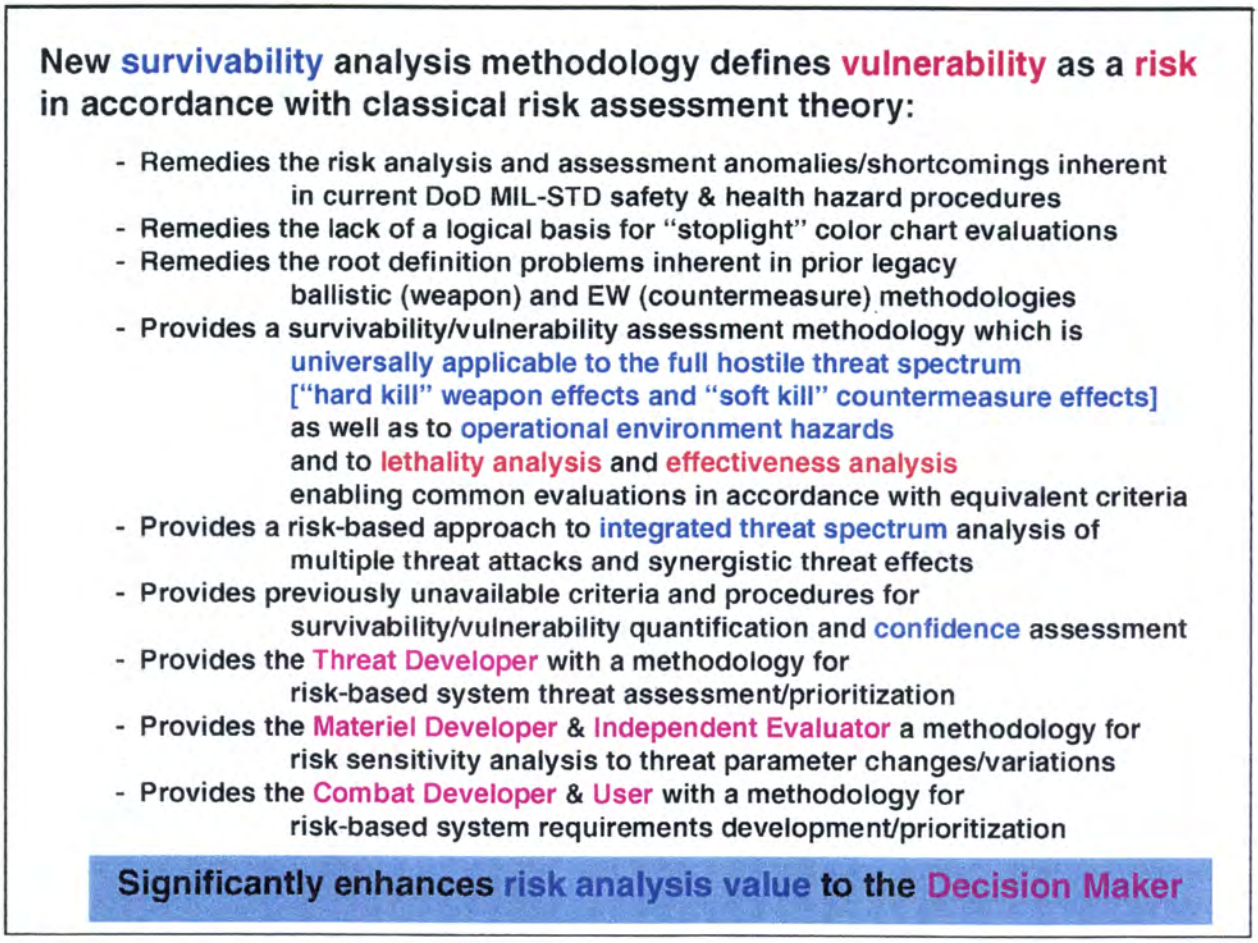

Figure 22. Vulnerability risk assessment methodology benefits.

References

1. Anon., Defense Acquisition, *DoD Directive 5000.1*, OSD, Washington, DC, Mar 96.

2. Anon., *Defense Acquisition Management Policies and Procedures*, DoD Instruction 5000.2, OSD, Washington, DC, Feb 91.

3. Anon., *Mandatory Procedures for Major Defense Acquisition Programs (MDAPs) and Major Automated Information System (MAIS) Acquisition Programs*, DoD Regulation 5000.2-R, OSD, Washington, DC, Mar 96.

4. Anon., *Vulnerability/Lethality Assessment*, AMC Reg 70-53, USAMC, Alexandria, VA, Dec 90.

5. Anon., *Risk Assessment Techniques (A Handbook for Program Management Personnel)*, ISI-V-3836-05, Defense Systems Management College, Ft Belvoir, VA, Jul 83.

6. Guzie, G.L., *The Application of Risk Assessment Theory to Countermeasure Vulnerability Assessment*, ARL-TR-1031, ARL/SLAD, WSMR, NM, Mar 97.

7. Anon., *Aircraft Survivability Terms*, MIL-STD-2089A, OSD, Washington, DC, Jul 81.

8. Anon., *ECCM: Electronic Warfare Susceptibility and Vulnerability*, AR 105-2, HQDA, Washington, DC, Nov 76.

9. Anon., *Electronic Warfare, Memo of Policy No. 6 (Rev 1)*, Chairman JCS, Washington, DC, Mar 93.

10. Anon., *Data Link Vulnerability Analysis (DVAL) Methodology*, USAF DVAL Joint Test Force, Kirtland AFB, NM, Nov 84.

11. Anon., *ECCM Requirements and Assessment Manual (ERAM)*, SECRET NF/WN, NWC Document 39-2196, Rev 6, Naval Air Warfare Center, China Lake, CA, Dec 92.

12. Anon., *Electronic Warfare Vulnerability Assessment Process Description*, Georgia Tech Research Institute, Atlanta, GA, Dec 91.

13. Anon., *System Safety Program Requirements*, MIL-STD-882C, OSD, Washington, DC, Jan 93.

14. Anon., *Procedures for Performing a Failure Mode, Effects, and Criticality Analysis (FMECA)*, MIL-STD-1629A, OSD, Washington, DC, Nov 80.

15. Anon., *National Missile Defense (NMD) System Threat Assessment Report (STAR)*, US Army Space and Missile Defense Command, Huntsville, AL, Dec 99.

Abbreviations and Acronyms

ATEC	Army Test & Evaluation Command
BMC3	battle management/command/control/communications
CCM	counter-counter measure
CM	countermeasure
DDT&E	Deputy Director, Test & Evaluation
DoD	Department of Defense
DVAL	data link vulnerability analysis
E3	electromagnetic environmental effects
ECCM	electronic counter-countermeasures
ECM	electronic countermeasures
EDWA	engagement decision & weapon assignment
EMI	electromagnetic interference
ERAM	ECCM requirements assessment manual
EW	electronic warfare
IOC	initial operational capability
IR	infrared
IW	information warfare
NMD	National Missile Defense
ORD	operational requirements document
OSD	Office of the Secretary of Defense
Penaid	penetration aid
RF	radio frequency
RSTA	reconnaissance, surveillance, & target acquisition

SEAD	suppression of enemy air defense
SSv	soldier survivability
STAR	system threat assessment report
TRADOC	Training and Doctrine Command
USAF	U.S. Air Force
USDR&E	Under Secretary of Defense, Research, & Engineering

Distribution

	Copies
SUITE 0944 8725 DEFENSE TECH INFO CTR DTIC OCA JOHN J KINGMAN RD FT BELVOIR VA 22060-6218	1
OFFICE SECY OF DEFENSE OUSD(A&T)/ODDR&E(R) DR R J TREW 3800 DEFENSE PENTAGON WASHINGTON DC 20301-3800	1
OUSD(A&T)/S&T AIR WARFARE MR R MUTZELBUG RM 3E139 3090 DEFENSE PENTAGON WASHINGTON DC 20310-3090	1
OUSD(A&T)/S&T LAND WARFARE MR A VIILU RM 3B1060 3090 DEFENSE PENTAGON WASHINGTON DC 20310-3090	1
OASD C3I MR J BUCHHEISTER RM 3D174 6000 DEFENSE PENTAGON WASHINGTON DC 20301-6000	1
UNDER SEC OF THE ARMY DUSA OR RM 2E660 102 ARMY PENTAGON WASHINGTON DC 20310-0102	1
ASST SEC ARMY ACQUISITION LOGISTICS & TECHNOLOGY SAAL ZD RM 2E673 103 ARMY PENTAGON WASHINGTON DC 20301-0103	1
ASST SEC ARMY ACQUISITION LOGISTICS & TECHNOLOGY SAAL ZP RM 2E661 103 ARMY PENTAGON WASHINGTON DC 20310-0103	1
ASST SEC ARMY ACQUISITION LOGISTICS & TECHNOLOGY SAAL ZS RM 3E448 103 ARMY PENTAGON WASHINGTON DC 20310-0103	1
OADCSOPS FORCE DEV DIR DAMO FDZ RM 31522 460 ARMY PENTAGON WASHINGTON DC 20310-0460	1

HQDA
ODCSPER
DAPE MR RM 2C733
300 ARMY PENTAGON
WASHINGTON DC 20301-0300 1

US MILITARY ACADEMY
MATH SCI CTR EXCELLENCE
MADN MSCE LTC M PHILLIPS
THAYER HALL
WEST POINT NY 10996-1786 1

US ARMY TRADOC
BATTLE LAB INTEGRATION
TECH & CONCEPTS DIR
ATCD B
FT MONROE VA 23651-5850 1

US ARMY TRADOC ANL CTR
ATRC W MR A KEINTZ
WSMR NM 88002-5502 1

DARPA
SPECIAL PROJECTS OFFICE
MR J CARLINI
3701 N FAIRFAX DR
ARLINGTON VA 22203-1714 1

ARMY EVALUATION CENTER
CSTE AEC MR W HUGHES
4120 SUSQUEHANNA AVE
APG MD 21005-3013 1

ARMY EVALUATION CENTER
CSTE AEC SV MR L DELATTRE
4120 SUSQUEHANNA AVE
APG MD 21005-3013 1

US ARMY MATERIEL CMD
DEP CHF OF STAFF FOR RDA
AMCRDA
5001 EISENHOWER AVE
ALEXANDRIA VA 22333-0001 1

US ARMY MATERIEL CMD
DEP CHF OF STAFF FOR RDA
AMCRDA T
5001 EISENHOWER AVE
ALEXANDRIA VA 22233-0001 1

US ARMY ARMAMENT RDEC
AMSTA AR TD MR M FISETTE
BLDG 1
PICATINNY ARSENAL NJ 07806-5000 1

SBCCOM RDEC
AMSSB RTD MR J ZARZYCKI
5183 BLACKHAWK RD
APG MD 21010-5424 1

US ARMY MISSILE RDEC
AMSMI RD DR W MCCORKLE
RSA AL 35898-5240 1

NATICK SOLDIER CENTER
SBCN T MR P BRANDLER
KANSAS STREET
NATICK MA 01760-5056 1

US ARMY TANK AUTOMTV RDEC
AMSTA TR MR J CHAPIN
WARREN MI 48397-5000 1

US AMRY INFO SYS ENGRG CMD
AMSEL IE TD DR F JENIA
FT HUACHUCA AZ 85613-5300 1

US ARMY SIM TRNG INST CMD
AMSTI CG DR M MACEDONIA
12350 RESEARCH PARKWAY
ORLANDO FL 32826-3726 1

US ARMY DEV TEST CMD
CSTE-DTC-TT-T
APG MD 21005-5055 1

DIRECTOR
US ARMY RESEACH OFFICE
4300 S MIAMI BLVD
RESEARCH TRIANGLE PARK NC 27709 1

US ARMY RESEARCH LAB
AMSRL DD DR J ROCCHIO
2800 POWDER MILL RD
ALDEPHI MD 20783-1197 1

US ARMY RESEARCH LAB
AMSRL SL DR J WADE
APG MD 21005-5068 1

US ARMY RESEARCH LAB
AMSRL SL MR J BEILFUSS
APG MD 21005-5068 1

US ARMY RESEARCH LAB
AMSRL SL E DR M STARKS
APG MD 21005-5068 1

US ARMY RESEARCH LAB
AMSRL SL EC MR E PANUSKA
APG MD 21005-5068 1

US ARMY RESEARCH LAB
AMSRL SL EM DR J FEENEY
APG MD 21005-5068 1

US ARMY RESEARCH LAB 1
AMSRL SL B MS J SMITH
APG MD 21005-5068

US ARMY RESEARCH LAB 1
AMSRL SL B MR J FRANZ
APG MD 21005-5068

US ARMY RESEARCH LAB 1
AMSRL SL B MR M VOGEL
APG MD 21005-5068

US ARMY RESEARCH LAB 1
AMSRL SL B MS W WINNER
APG MD 21005-5068

US ARMY RESEARCH LAB 1
AMSRL SL BA MS M RITONDO
APG MD 21005-5068

US ARMY RESEARCH LAB 1
AMSRL SL BD MR J MORRISSEY
APG MD 21005-5068

US ARMY RESEARCH LAB 1
AMSRL SL BE MR D BELY
APG MD 21005-5068

US ARMY RESEARCH LAB 1
AMSRL SL BG MS A YOUNG
APG MD 21005-5068

US ARMY RESEARCH LAB 1
AMSRL SL BN MR D FARENWALD
APG MD 21005-5423

US ARMY RESEARCH LAB 1
AMSRL SL MR C HOPPER
WSMR NM 88002-5513

US ARMY RESEARCH LAB 1
AMSRL SL E MR J PALOMO
WSMR NM 88002-5513

US ARMY RESEARCH LAB 1
AMSRL SL EA MR R FLORES
WSMR NM 88002-5513

US ARMY RESEARCH LAB 1
AMSRL SL EI MR J NOWAK
FT MONMOUTH NJ 07703-5601

US ARMY RESEARCH LAB 1
AMSRL CS AS
2800 POWDER MILL RD
ADELPHI MD 20783-1197

US ARMY RESEARCH LAB AMSRL CS EA TP 2800 POWDER MILL RD ADELPHI MD 20783-1197	3
US ARMY RESEARCH LAB AMSRL CI LL 2800 POWDER MILL RD ADELPHI MD 20783-1197	3
US ARMY RESEARCH LAB AMSRL CI LP BLDG 305 APG MD 21005-5068	2
US ARMY RESEARCH LAB AMSRL SL EA MR G GUZIE WSMR NM 88002-5513	10
Record copy	1
Total	67